Canadian Information Processing Society-L'Association Canadienne de l'Informatique

Canada's Association of Information Technology Professionals

Submission

To the Office of the Privacy Commission of Canada

Proposals for ensuring appropriate regulation of artificial intelligence

Respectfully Submitted: March 13, 2020

Executive Summary

Canadian Information Processing Society - L'Association Canadienne de l'Informatique (CIPS/ACI) is the national association for Information Systems professionals in Canada.

CIPS believes that universal protection of personal information is fundamental to the effective application of IT (Information Technology) in all domains that use personal information. Only when individuals trust their personal information will be used for their own interests, and protected from inappropriate use and disclosure, can there be any expectation that they will provide complete and accurate disclosure of that information. And reliable information is foundational to information systems that serve individuals and society effectively, accurately, and safely.

CIPS agrees with the OPC that consent no longer provides a satisfactory foundation to support authorized and appropriate use of personal information. We believe integration of protection of personal information into design specifications, business practices, IT operational practices, and the associated audits, is the only way to ensure that personal information is protected as information technology and systems continue their expansion and rapid rate of change.

CIPS, through its Code of Ethics, has a long history of advocating this position.

CIPS would ask that an exploration of the option of applying the principles of licensed professional practice to the practice of Information Systems in the processing of personal information be included in this consultation.

Both CIPS, and the OPC, has identified that the application of information technology without consideration of its impact to personal privacy is the fundamental enabler of loss of personal privacy. CIPS asks for the opportunity to explore how Information Systems practitioners can be engaged as a solution to these challenges, rather than enablers of the issue.

Table of Contents

Introduction

Introduction to CIPS/ACI

CIPS/ACI is Canada's association of information systems professionals, representing practitioners on issues affecting the profession and industry. CIPS is involved in a number of initiatives related to public policy, setting standards within the information systems profession, and assisting its community.

Our main programs are:

- Certification of information systems professionals;
- Accreditation of computer science, software engineering, and management information systems programs in colleges and universities; and
- Professional development of our membership through presentations, educational events, and conferences.

History

In September 1958 a group of Data Processing workers got together to talk about common concerns. That conference demonstrated to participants the value of sharing ideas, networking with fellow professionals, and learning about changes in the technology, practices, and management of information systems.

This event sparked the formation of the Computing and Data Processing Society of Canada.

In 1968, the society changed its name to the Canadian Information Processing Society (CIPS).

In 1989, CIPS established the Information Systems Professional (I.S.P.) designation.

Today CIPS represents thousands of information systems professionals across Canada.

Certified Information Systems Professionals

CIPS has several membership categories. For those members who have met the requirements of education and experience necessary to be registered as a certified member, CIPS awards the designation of Information Systems Professional (I.S.P.).

All CIPS members must:

- Abide by the CIPS Code of Ethics.
- Practice only within their areas of competency; and
- Remain current with the advances in the field.

Certified members are answerable to their peers through a formal disciplinary process.

The I.S.P. features flexibility to information systems practitioners, and organizations that hire and/or contract information systems practitioners as it:

- can be secured through a range of options including education, experience, and testing
- is available to, is held by, and relevant to, the entire range of IT practitioners from primary support providers to senior management; and
- is available, and supported by, CIPS bodies across Canada.

The CIPS Code of Ethics

Distinguishing marks of a profession are its acceptance by the public, and the profession's acceptance of its responsibility to the public. The following statements are a set of high ideals to which all CIPS members aspire. CIPS members have an obligation to:

- Imperative #1: Protect the Public Interest and Privacy of Information
  Carry out work or study with primary regard for public interest (including health, security, safety, privacy, protection of the environment and social responsibility) and in accordance with regulatory requirements and legislation.
- Imperative #2: Avoid Conflicts of Interest
  Act so the welfare of others takes precedence over personal interests and provide full disclosure to impairment of personal judgment.
- Imperative #3: Take Professional Responsibility
  Serve their employer/clients competently, carry out their work with due diligence, maintain and advance their knowledge and exercise uncompromised professional judgment.
- Imperative #4: Contribute to the IT Profession
  Respect the rights and professional aspirations of colleagues and uphold the integrity, dignity and image of the profession.

CIPS members are expected to be familiar with and to not act contrary to the Code. CIPS members assume an obligation of integrity above and beyond the requirements of laws. Unless stated, the Code applies equally to both certified and non-certified members.

Lack of awareness does not excuse unethical behaviour; violators may be subject to disciplinary actions including but not limited to suspension or termination of membership and/or professional certification. CIPS members are obligated to report unethical behavior or violation of the Code by other CIPS members.

Outline of our submission

CIPS submission to the Office of the Privacy Commissioner of Canada in response to "Proposals for ensuring appropriate regulation of artificial intelligence" includes the following:

- Background
- Response to the Proposals for Consideration
- Offer of support

The Background section provides an overview of the personal information domain that supports our responses to the discussion questions.

Our Response to the Proposals for Consideration provides CIPS responses to the questions asked in the “Consultation on the OPC’s Proposals for ensuring appropriate regulation of artificial intelligence”. We have limited our responses to those questions that, in our interpretation, include a specific component related to the practice of information systems, or where the domain of information technology has a particular contribution to make. CIPS anticipates other groups and individuals who have specific knowledge in the domains where we have chosen not to comment will provide input on these points. We look forward to reviewing these responses and providing feedback where appropriate.

The Offer of Support outlines CIPS's commitment to work with the Office of the Privacy Commissioner of Canada on this and any other topic where our participation may be of value.

Background

The relationship between protection of personal information and the practice of information systems

The necessity to provide protections related to the collection, use, and disclosure of personal information is directly driven by, and intimately related to, the practice of information systems.

Before the widespread adoption of automated information technology manual labour and associated costs to access, correlate, and physically copy or relocate records generally limited the access and disclosure of personal records to their original purpose. But once personal information is managed by automated systems it can inexpensively be shared within, and among, organizations and individuals, facilitating application of personal information outside of the purpose and context for which it was collected.

It becomes possible, through correlation of personal information provided in good faith, independently to different organizations and in diverse contexts, to derive new information about identifiable individuals. In many cases the individual is not privy to, nor was prepared to disclose, this information.

Good information technology practices are fundamental to ensure protection of personal information. Without appropriate IT practices (e.g. identity management, access control, encryption, intrusion detection) the most noble of objectives for the protection of personal information protection can neither be implemented nor assured. And it is only through the integration of personal information protection principles with information systems design and operating procedures that personal information will continue to be protected as new technologies and processes are implemented.

Changes in information technology that impact the use of personal information
There have been significant changes in information technology since the principles of personal information protection were established.

In 2003, for most citizens collection of personal information was the result of initiating a transaction, in person, at an organization's physical place of operation. Paper documents were the authoritative and complete record of personal information and only certain data like banking transactions were recorded in on-line systems. Interaction with organizations other than in person or by telephone was rare, and typically only involved preliminary research or information gathering.

In 2020 most organizations no longer rely on paper records of personal information. All personal information is recorded in information systems. These systems now include data types such as images, and likely include a complete and detailed history of an individual's interaction with the organization. In many cases the organization will also hold personally identifiable information that was not disclosed by the individual to the organization, such as data derived from services that track on-line activity or was provided by a social media site.

In 2003, only large organizations used information systems to collect and use personal information. Today all organizations, both large and small, for profit and non-profit, manage personal information with information systems. Smaller organizations rarely have personnel charged with ensuring appropriate practices related to the personal information they hold.

In many cases an individual's interaction with an organization will now occur only through interaction with information systems. Many organizations actively discourage, or prevent, in-person dealings with the organization. With the burden of data entry passed from the organization to the customer there is no cost disincentive to collect personal information that is peripheral to the transaction.

In 2003, it cost millions of dollars to store the personal information held by a large organization. Significant stores of personal information were managed and protected by professional information systems practitioners.

Today a few hundreds of dollars will buy enough storage to make a copy of the personal information held by even the largest of organizations. As a result of well-meaning initiatives, and malicious intent, copies of personal information can easily move from professionally managed systems to ad hoc copies that are no longer under the control of the organization.

Much of the cost “friction” to the use of personal information has been eliminated. Organizations are incentivized to collect and retain personal information even if the value of any individual record is minimal, as the cost of retaining and processing the record is so low that there can still be a return.

In 2003 a communications device that was dedicated to an individual, always in physical proximity to its owner, and which could collect data autonomously, was rare. Mobile phones were typically used for voice communications only. Few homes would have had more than a single shared personal computer. Unless an individual voluntarily and explicitly identified themselves, anonymity could be presumed.

In 2020, most access to on-line services is through a device that is uniquely and reliably associated with an individual, i.e. a tablet or smart telephone. These devices can reliably detect, record, and disclose personally identifying information such as location, usage patterns, and physical activity. When combined with web analytics systems, the reality is that an organization often holds personal information about an individual even if the individual has never initiated a formal relationship with that organization.

Data collection capability has been added to products that most consumers would not associate with the collection of personal information. Intelligent thermostats allow the user to remotely change the temperature of their home, keep the manufacturer up to date on the user's whereabouts, and report whether the house is occupied. Smart televisions report the viewer's detailed viewing history, and collect and transmit every sound in the room to a remote server. The processing capability, network connectivity, and absence of typical information system practices such as monitoring and software updates make these devices highly attractive targets for malicious activity.

Low cost telecommunications mean that information services can be acquired largely without consideration of location. This has cost advantages through the use of lower cost labour and

energy, and the application of extreme economies of scale. However it means that traditional protections of law and legal process, which are based on political geography, cannot be relied upon to protect personal information.

Going forward, there is no indication that this rate of change will cease. Emerging technologies such as advanced machine learning and artificial intelligence (AI) will provide further incentives for organizations to collect and use personal information.

Given the even more significant changes in, and broader applications of, information systems likely in the next 10 years, CIPS suggests that a more proactive, professional practice based solution to the protection of personal information is required.

Responses to the Proposals for Consideration

Proposal 1: Incorporate a definition of AI within the law that would serve to clarify which legal rules would apply only to it, while other rules would apply to all processing, including AI

CIPS Response:
AI as outlined in the consultation is a form of information processing. CIPS does not support the concept of technology-specific safeguards. Fundamentally, many concepts presented as new "technologies" are simply re-packaging and re-labelling of established information technology processes and principles. Specific to AI, the consultation outlines that "[the OPC is] paying specific attention to AI systems given their rapid adoption for processing and analysing large amounts of personal information" and "their use for making predictions and decisions affecting individuals may introduce privacy risks as well as unlawful bias and discrimination." These statements could have been made in 1980 about information systems generally and still can. Any legal rules should apply to all information processing.

Discussion questions:

Should AI be governed by the same rules as other forms of processing, potentially enhanced as recommended in this paper (which means there would be no need for a definition and the principles of technological neutrality would be preserved) or should certain rules be limited to AI due to its specific risks to privacy and, consequently, to other human rights?

CIPS Response:
AI should be governed by the same rules as other forms of information processing. CIPS supports the principles of technological neutrality and there is no need for a definition of artificial intelligence.

If certain rules should apply to AI only, how should AI be defined in the law to help clarify the application of such rules?

CIPS Response:
There should be no rules that apply to AI only.

Proposal 2: Adopt a rights-based approach in the law, whereby data protection principles are implemented as a means to protect a broader right to privacy—recognized as a fundamental human right and as foundational to the exercise of other human rights

CIPS Response:
CIPS recommends seeking advice from The Federation of Law Societies of Canada on the topic of the law and the Privacy and Access Council of Canada on the topic of privacy.

Discussion question

What challenges, if any, would be created for organizations if the law were amended to more clearly require that any development of AI systems must first be checked against privacy, human rights and the basic tenets of constitutional democracy?

CIPS Response:
Establishing a concise, universal, and enforceable list of requirements respecting privacy, human rights, and democracy is not achievable. It is impossible to conceive of an approach that will articulate the all the potential uses of an individual's personal information, and the potential impact of those uses on an individual's privacy, yet remains concise and readable enough that a cursory reading, let alone any comprehensive understanding, is achievable within the practical cost and time constraints of most business services, processes, or transactions.

We would suggest that pursuing further refinements in privacy policy related to artificial intelligence specifically has the potential to consume resources, and apply friction to commercial and civic transactions, with little, if any, impact on the actual protection of individuals personal information.

CIPS believes that any sustainable solution to the protection of personal information and individual privacy must recognize this reality. Determination of whether a particular act of processing that involves personal information is appropriate is, and will always remain, a complex act that requires proven competency in practice, sensitivity to context, and the application of professional judgement.

Processing of personal information is not unique in this regard. There are many endeavours that society rely upon where complexity of the domain, ongoing advancements in practice, and the limited capacity of the non-practitioner to provide oversight, makes regulation impractical to ensure that practices in the domain respect the integrity of the client or customer, and are executed to the interests of the broader public good. In these cases a self regulated professional practice, accountable for ensuring the practice is applied to the broad public good, is the preferred solution.

Most of the issues with protection of personal information come about because there is a divergence between private interests of a custodian of personal information, and the benefit, and potential harm, to the individual whose personal information is being processed.
This is a long-standing issue in many other domains. The solution has consistently been professional practitioners, with a degree of control over their practice independent from their employer, who are accountable to their peers for the outcome of their actions.

Effective protection for personal information will come about only when ownership of the principles, practices, and outcomes related to the protection of personal information are integrated with the other practices and principles that constitute the professional practice of Information Systems.

We believe the way forward is for the information systems profession, working in an ongoing partnership with existing privacy policy and regulatory bodies, to establish a professional practice of Information Systems where protection of personal information is a key accountability.

CIPS cannot identify another domain of similar size, complexity, or impact, as Information Systems where imposition of practices from outside the domain, without either authority over practitioners, nor accountability for outcomes, is considered an acceptable solution. We see no reason why Information Systems should be treated any differently than any other complex endeavour where mastery of practice, and ongoing sophisticated decision making, is required to achieve a desired societal outcome.

Proposal 3: Create a right in the law to object to automated decision-making and not to be subject to decisions based solely on automated processing, subject to certain exceptions

CIPS Response:
We believe that accountability for decision-making must be placed clearly and unequivocally with the organizations that collect and use personal information, and the Information Systems practitioners who enable those processes. Ultimately, “automated decision-making” does not exist - Information Systems practitioners have used technology, like AI, to enable business processes in accordance with the requirements of their employers.

Discussion questions

Should PIPEDA include a right to object as framed in this proposal?

CIPS Response:
CIPS agrees that a right to object and to be free from “automated decisions” as analogous to the right to withhold consent in the sense that consent must be granted before processing personal information. CIPS does not see a distinction between “automated decisions” and

decisions. Ultimately, the organization must be held accountable and so must the Information Systems practitioners.

If so, what should be the relevant parameters and conditions for its application?

CIPS Response:
We suggest that the conditions where individuals and organizations are accountable for ensuring protection of personal privacy in all contexts is the best way forward. There is more value in the approach suggested in the White House Report *Big Data: Seizing Opportunities, Preserving Values*.

Simply put, an individual's personal information should be collected and used for those purposes related to the context in which it was collected. Disclosure and use outside of that context should be done only where there is justifiable, socially beneficial, value to be derived. All use outside of that, including for personal or organizational economic gain, should be prohibited except where informed consent has been secured.

Proposal 4: Provide individuals with a right to explanation and increased transparency when they interact with, or are subject to, automated processing

CIPS Response:
CIPS maintains that "automated" processing is no different from general information processing. An organization must be held accountable for their decisions, the factors involved in the decision, and provide logic upon which the decision is based if the decision is impactful. These may eventually be automated through technology by an Information Systems practitioner. Both the organization and the Information Systems practitioner must be held accountable.

Transparency requirements for both the organization and the Information Systems practitioner could be established, regardless of whether processing is "automated". As noted above, however, establishing a concise, universal, and enforceable list of requirements is not achievable. A preferred solution would be a self regulated professional practice, accountable for ensuring the practice is applied to the broad public good.

Discussion questions

What should the right to an explanation entail?

CIPS Response:
OPC notes that “a right to explanation that would provide individuals interacting with AI systems the reasoning underlying any automated processing of their data, and the consequences of such reasoning for their rights and interests” but CIPS does not see a reason why this should apply to “AI” systems only.

Would enhanced transparency measures significantly improve privacy protection, or would more traditional measures suffice, such as audits and other enforcement actions of regulators?

CIPS Response:
CIPS suggests that additional regulatory powers, and new or enhanced rules for transparency or otherwise, will do little to advance protection of Canadian's personal information.

The primary impediment to regulation as a route to protecting personal information is the fundamental lack of transparency in the acts and outcomes. It can be difficult for specialists in the field to make a quick and definitive determination as to whether any particular act of acquiring or processing personal information is inappropriate. It is impossible for the non-practitioner to make that determination.

When there has been an inappropriate use of personal information, the evidence of such rarely leaves the organization involved. What evidence, if any, that can be found of inappropriate use of personal information is usually circumstantial and difficult, if not impossible, to trace back to the responsible party.

As a result only the most egregious and public instances of failures in protection of personal privacy are identified, investigated, and enforced.

Unfortunately, this does little to ensure Canadian's individual privacy. Our privacy is not lost as a result of a few malicious or incompetent actions. It is lost as a result of the hundreds of thousands of incidents of collection and use, often without consent, of our personal information that while, perhaps individually well intended and inconsequential, can be assembled and correlated to result in complete loss of an individual's privacy.

And given the substantial returns to be derived from the acquisition and use of personal information, and the limited possibility of censure from inappropriate use, the risk vs. reward calculation is straightforward for most organizations.

The challenge for regulators is that, almost universally, the assessment process is instigated on a complaint basis. But in this domain the harmed individual(s) will only in the most exceptional circumstances become aware that their personal information was inappropriately used. Even if they do become aware their privacy has been compromised, identifying the custodian responsible will be difficult.

The alternative is involuntary auditing of custodian organizations. While this is applied in some select domains (e.g. finance), most organizations would object significantly to the intrusion and additional cost.

A regulatory approach primarily addresses failures in the protection of personal information after the fact. This is of little value to the impacted individuals, as the harm cannot be undone. We believe that a proactive approach, with a focus on establishing practices that prevent failures in the protection of personal information in the first place, is of more value.
We believe the resources required to establish and sustain a regulatory regime would be better applied to working with the Information Systems profession to establish practice guidelines, enhance the body of knowledge in the field, and ensuring that the professional self-regulatory accountability is being discharged.

Proposal 5: Require the application of Privacy by Design and Human Rights by Design in all phases of processing, including data collection

CIPS Response:
We believe that Privacy by Design needs to be a requirement for all systems that collect and use personal information, and needs to become as fundamental to information systems practice as existing practices of security and reliability.

Discussion questions

Should Privacy by Design be a legal requirement under PIPEDA?

CIPS Response:
We believe ensuring personal privacy is fundamental to professional business and information technology practices.

Privacy by Design cannot be simply encouraged. Otherwise, organizations that incur the higher operating costs, lost income from the sale of personal information, reduced marketing opportunities, and increased administrative burden, of effective privacy practices will be at a disadvantage to those organizations who do not embrace these practices.

CIPS would suggest the way to achieve this integration is not through direct legislation and regulation of practices. Rather, as with other complex domains where it is unreasonable to expect the layman user of services to be able to effectively evaluate the impact of a practitioners actions, the way to achieve Privacy by Design is to make it part of the broad range of competencies and ethical commitments provided by professional practitioners in Information Systems.

Would it be feasible or desirable to create an obligation for manufacturers to test AI products and procedures for privacy and human rights impacts as a precondition of access to the market?

CIPS Response:
CIPS does not see a reason why this should apply to "AI" products and procedures only. As noted above, however, establishing a concise, universal, and enforceable list of requirements is not achievable. A preferred solution would be a self regulated professional practice, accountable for ensuring the practice is applied to the broad public good.

Proposal 6: Make compliance with purpose specification and data minimization principles in the AI context both realistic and effective

CIPS Response:
Purpose specification and data minimization are still applicable in the AI context. CIPS maintains that AI is no different from general information processing.

Discussion questions

Can the legal principles of purpose specification and data minimization work in an AI context and be designed for at the outset?

CIPS Response:
Yes. CIPS maintains that AI is no different from general information processing. If there is a requirement, legal or otherwise, for purpose specification and data minimization, then that requirement can be accommodated.

If yes, would doing so limit potential societal benefits to be gained from use of AI?

CIPS Response:
Most of the issues with protection of personal information come about because there is a divergence between private interests of a custodian of personal information, and the benefit,

and potential harm, to the individual whose personal information is being processed and the community or society at large to which they belong.

This is a long standing issue in many other domains. The solution has consistently been professional practitioners, with a degree of control over their practice independent from their employer, who accountable to their peers for the outcome of their actions.

Proposal 7: Include in the law alternative grounds for processing and solutions to protect privacy when obtaining meaningful consent is not practicable

CIPS Response:
Consent no longer provides a satisfactory foundation to support authorized and appropriate use of personal information.

The concept of using consent as the enabling authorization for the collection, use and disclosure of personal information arose largely because establishing a concise, universal, and enforceable statement of authorization for the use of personal information that maintains individual privacy, while enabling effective commerce and civic operations, is not achievable.

CIPS believes that any sustainable solution to the protection of personal information and individual privacy must recognize this reality. Determination of whether a particular act of processing that involves personal information is appropriate is, and will always remain, a complex act that requires proven competency in practice, sensitivity to context, and the application of professional judgement.

The processing of personal information is not unique in this regard. There are many endeavours that society rely upon where complexity of the domain, ongoing advancements in practice, and the limited capacity of the non-practitioner to provide oversight, makes regulation impractical to ensure that practices in the domain respect the integrity of the client or customer, and are executed to the interests of the broader public good. In these cases a self regulated professional practice, accountable for ensuring the practice is applied to the broad public good, is the preferred solution.

Most of the issues with protection of personal information come about because there is a divergence between private interests of a custodian of personal information, and the benefit, and potential harm, to the individual whose personal information is being processed.
But this a long standing issue in many other domains. And the solution has consistently been professional practitioners, with a degree of control over their practice independent from their employer, who accountable to their peers for the outcome of their actions.

Effective protection for personal information will come about only when ownership of the principles, practices, and outcomes related to the protection of personal information are integrated with the other practices and principles that constitute the professional practice of Information Systems.

We believe the way forward is for the information systems profession, working in an ongoing partnership with existing privacy policy and regulatory bodies, to establish a professional practice of Information Systems where protection of personal information is a key accountability.

CIPS cannot identify another domain of similar size, complexity, or impact, as Information Systems where imposition of practices from outside the domain, without either authority over practitioners, nor accountability for outcomes, is considered an acceptable solution. We see no reason why Information Systems should be treated any differently than any other complex endeavour where mastery of practice, and ongoing sophisticated decision making, is required to achieve a desired societal outcome.

Discussion questions

If a new law were to add grounds for processing beyond consent, with privacy protective conditions, should it require organizations to seek to obtain consent in the first place, including through innovative models, before turning to other grounds?

CIPS Response:
The concept of using consent as the enabling authorization for the collection, use and disclosure of personal information arose largely because establishing a concise, universal, and enforceable statement of authorization for the use of personal information that maintains individual privacy, while enabling effective commerce and civic operations, is not achievable. Obtaining consent should not be the default mechanism in every case.

Determination of whether a particular act of processing that involves personal information is appropriate is, and will always remain, a complex act that requires proven competency in practice, sensitivity to context, and the application of professional judgement.

Is it fair to consumers to create a system where, through the consent model, they would share the burden of authorizing AI versus one where the law would accept that consent is often not practical and other forms of protection must be found?

CIPS Response:

Most consumers have little awareness of, and therefore make no consideration of, compromises to their individual privacy when making acquisition decisions. As a result the organization that applies rigorous controls to personal information is at a cost disadvantage to their competitors, and receives no consideration in return.

Achieving effective protection of Canadians personal privacy will require the establishment of three conditions:

- protection of personal privacy becomes a fundamental tenet and requirement of IT practice
- protection of personal privacy becomes a consideration of individuals when selecting service offerings
- businesses are recognized and rewarded for service offerings and practices that maintain personal privacy

There are many precedents where society has enforced consistency, transparency, and ethicality across all practitioners in a domain in order to establish that harm to the individual is never an unacceptable outcome when the interests of the individual and the organization diverge. CIPS sees no reason why this precedent should not apply in the domain of Information Systems practice related to personal information.

Requiring consent implies organizations are able to define purposes for which they intend to use data with sufficient precision for the consent to be meaningful. Are the various purposes inherent in AI processing sufficiently knowable so that they can be clearly explained to an individual at the time of collection in order for meaningful consent to be obtained?

CIPS Response:
CIPS makes no distinction between AI and information processing. An individual's personal information should be collected and used for those purposes related to the context in which it was collected. Disclosure and use outside of that context should be done only where there is justifiable, socially beneficial, value to be derived. All use outside of that, including for personal or organizational economic gain, should be prohibited except where informed consent has been secured.

What are your views on adopting incentives that would encourage meaningful consent models for use of personal information for business innovation?

CIPS Response:
CIPS cannot conceive of an incentive based mechanism that would be effective.

Proposal 8: Establish rules that allow for flexibility in using information that has been rendered non-identifiable, while ensuring there are enhanced measures to protect against re-identification

CIPS Response:
CIPS takes the position that there are no reliable criteria to assess the risk of re-identification. Any data set that retains useful information is, given current processing capacity and analytical tools and the ready availability of large data sets that can be used for correlation, at significant risk of re-identification.

There will be a tendency to relax the controls and protections applied to a de-identified data set under the assumption that the data cannot be re-identified. Since that assertion cannot be guaranteed, we believe that personal data should be retained in its original state and that rigorous controls should be applied in perpetuity.

Discussion questions

What could be the role of de-identification or other comparable state of the art techniques (synthetic data, differential privacy, etc.) in achieving both legitimate commercial interests and protection of privacy?

CIPS Response:
Any data set that retains useful information is, given current processing capacity and analytical tools and the ready availability of large data sets that can be used for correlation, at significant risk of re-identification, regardless of the technology or technique used to de-identify.

Which PIPEDA principles would be subject to exceptions or relaxation?

CIPS Response:
We do not believe that any relaxation or exceptions are warranted at this time.

What could be enhanced measures under a reformed Act to prevent re-identification?

CIPS Response:
Large amounts of personally identifying information are collected and used, without consent that could be considered “de-identified data” from their origin. For example, location and movement of cell phones is tracked through their SSID and MAC addresses. This data can be correlated with other data sources to reliably track individuals.

Allowing for the collection, use and disclosure of de-identified data without consent under any context will encourage these data sets being held without the effective controls and practices necessary to ensure ongoing protection of personal information. Some measures to prevent this should be considered.

Proposal 9: Require organizations to ensure data and algorithmic traceability, including in relation to datasets, processes and decisions made during the AI system lifecycle

CIPS Response:
CIPS makes no distinction between AI and information processing. For an organization and the Information Systems practitioner to be held accountable, being able to trace how decisions are arrived at through the supporting business processes is necessary, regardless of whether they are automated or not.

Discussion question

Is data traceability necessary, in an AI context, to ensure compliance with principles of data accuracy, transparency, access and correction and accountability, or are there other effective ways to achieve meaningful compliance with these principles?

CIPS Response:
Data traceability is necessary for compliance purposes, whether in an AI context or not. CIPS maintains that AI is analogous with information processing.

Proposal 10: Mandate demonstrable accountability for the development and implementation of AI processing

CIPS Response:
Liability or accountability can never be held by information systems, within an AI context or otherwise. Liability must be held by the organization or by the Information Systems practitioner.

Integrating the protection of personal information with the professional practice of Information Systems would bring to bear the broad range of support services and practices that supports sophisticated decision making, such as:

- common body of knowledge
- ongoing professional development
- peer consultation and advisement
- ongoing practice reviews

Placing the accountability with the professional practitioner is the best way to ensure that the sophisticated decision making required is applied consistently across all custodians of personal information, and ensuring that the decisions are made based upon principles of personal privacy protection, rather than the self interest of the custodian organization.

Discussion questions

Would enhanced measures such as those as we propose (record-keeping, third party audits, proactive inspections by the OPC) be effective means to ensure demonstrable accountability on the part of organizations?

CIPS Response:
The challenge to using regulators for the purpose of accountability is that, almost universally, the assessment process is instigated on a complaint basis. In this domain the harmed individual(s) will only in the most exceptional circumstances become aware that their personal information was inappropriately used. Even if they do become aware their privacy has been compromised, identifying the custodian responsible will be difficult.

The alternative is involuntary auditing of custodian organizations. While this is applied in some select domains (e.g. finance), most organizations would object significantly to the intrusion and additional cost.

A regulatory approach primarily addresses failures in the protection of personal information after the fact. This is of little value to the impacted individuals, as the harm cannot be undone. We believe that a proactive approach, with a focus on establishing practices that prevent failures in the protection of personal information in the first place, is of more value.

We believe the resources required to establish and sustain a regulatory regime would be better applied to working with the Information Systems profession to establish practice guidelines, enhance the body of knowledge in the field, and ensuring that the professional self-regulatory accountability is being discharged.

What are the implementation considerations for the various measures identified?

CIPS Response:
CIPS cannot conceive of a method by which any of these measures could be effective without a situation where the individuals involved were not supported by the ongoing professional education, opportunity for peer consultation and review, and professional accountability for, and independence of practice, that come from professional practitioners doing the work involved making, or supporting, these decisions.

We believe a much better approach would be to establish effective and responsive mechanisms to support the Information Systems practitioner in quickly making effective and ethical decisions. These mechanisms would include:

- Ongoing professional development
- Access to peers for consultation and review
- Contribution to, and usage of, accepted bodies of knowledge

We believe this approach would provide much more effective, timely, and cost effective decision making which, because it is integrated into the activities required to complete the processing of the personal information, has a much higher probability of being consistently applied.

The costs of these services would be included with the fees associated with the operation of the professional association, and would therefore be directly and proportionally allocated to the organizations and individuals who make use of personal information.

What additional measures should be put in place to ensure that humans remain accountable for AI decisions?

CIPS Response:
CIPS believes the vital role of the OPC, and her or his provincial counterparts, in policy research and development and ensuring compliance to relevant legislation and regulation, remains.

However, we would propose that primary accountability for ensuring individual privacy is maintained will be achieved only by integrating this requirement with the practice of Information Systems as it is applied to the processing of personal information. It is through a partnership where the OPC and its provincial counterparts provide policy, guidance, and oversight, and the Information Systems profession holds accountability for execution and outcome, that Canadians personal privacy can be assured.

As labour is a provincial responsibility, legislation specifying professional certification requirements for particular areas of activity would have to be implemented at that level.

Proposal 11: Empower the OPC to issue binding orders and financial penalties to organizations for non-compliance with the law

CIPS Response:
CIPS agrees that to incentivize compliance with the law, PIPEDA must provide for meaningful enforcement with real consequences for organizations found to be non-compliant.

Discussion questions

Do you agree that in order for AI to be implemented in respect of privacy and human rights, organizations need to be subject to enforceable penalties for non-compliance with the law?

CIPS Response:
Yes, organizations need to be subject to enforceable penalties for non-compliance with the law.

The motivations are compelling for business to acquire, and make broad use of, personal information. It could be argued that organizations who are prepared to offer exceptional protection to personal privacy (i.e. acquire and use personal information strictly on the basis of consent, as per existing Canadian privacy law) are no longer viable in the face of competition, particularly from outside of Canada, who apply less discretion in their acquisition and application of personal information.

Many services are offered where the charges to the individual do not reflect the actual cost required to sustainably provision the service. In many cases, no charge at all is levied to the individual user.

The primary revenue to the operators of these services comes from sale of targeted marketing and sales opportunities to other organizations, based on examination of the information collected by the service from the individuals using the service.

It is understandably compelling for individuals to prefer service offerings that are funded by the sale of the individual's information rather than fees paid by them directly. But CIPS would argue that most individuals using these services do not appreciate the compromises to their personal privacy that arise from using these services.

A concern of CIPS is that these "free" services are so compelling that they are, for most individuals, pushing other alternatives out of practical availability. As a result it is becoming

difficult, if not impossible, to function in society while retaining absolute control over one's personal information.

Even for organizations who are not involved with the direct offer of digital services there is tremendous motivation to use, and disclose, personal information outside the context for which it is collected and used.

CIPS would argue that it is eminently impractical, and unfair, to expect business to self regulate their use of individual's personal information in the current context. Most consumers have little awareness of, and therefore make no consideration of, compromises to their individual privacy when making acquisition decisions. As a result the organization that applies rigorous controls to personal information is at a cost disadvantage to their competitors, and receives no consideration in return.

Achieving effective protection of Canadians personal privacy will require the establishment of three conditions:

- protection of personal privacy becomes a fundamental tenet and requirement of IT practice
- protection of personal privacy becomes a consideration of individuals when selecting service offerings
- businesses are recognized and rewarded for service offerings and practices that maintain personal privacy.

There are many precedents where society has enforced consistency, transparency, and ethicality across all practitioners in a domain in order to establish that harm to the individual is never an unacceptable outcome when the interests of the individual and the organization diverge. CIPS sees no reason why this precedent should not apply in the domain of Information Systems practice related to personal information.

Are there additional or alternative measures that could achieve the same objectives?

CIPS Response:
An effective privacy policy must:

- be owned by, and provide value to, the individuals and organizations charged with its implementation and ongoing integrity
- demonstrate independence and objectivity in motivation, objectives, processes, and investigation and dispute mechanisms
- be entirely transparent and accountable in all aspects of its operation

These requirements have exact parallels to those that have led to regulated professional practice. Certifications of institutions and practices are established precedent when execution of a complex practice to the broader public good is necessary.

We believe that the best way forward is for PIPEDA to continue to provide the policy level guidance for protection of personal information and the regulatory mechanisms required for investigation and resolution of exceptional circumstances.

The operational accountability for protection of personal information should become a mandatory, enforceable, accountability of all Information Systems practitioners who deal with personal information, as it is for I.S.P. holders today.

Conclusion

CIPS would like to thank the Office of the Privacy Commissioner of Canada for their attention to our submission and the opportunity to contribute to this review.

CIPS looks forward to continuing to work with the Government of Canada to improve the protection of Canadian's personal information.

Offer of Support

As the national professional association for information systems practitioners, CIPS can engage and mobilize information systems professionals across all IT domains. This includes senior business IT leaders, owners and managers of IT service providers, Academic leaders and practitioners, and senior experts in all fields of IT.

We welcome any opportunity to assist the Government of Canada in any way we may be of assistance.

Authorship

This document was prepared by Derek Burt, I.S.P., ITCP based on input from a previous consultation with:

Mark Olson, I.S.P., ITCP
Kerry Augustine, I.S.P., ITCP
Dr. Lee Anne Davies, MA, MBA, PhD
Doran Ingalls, LLB, Former Secretary of CIPS Alberta
David PJ O'Leary I.S.P., I.T.C.P./IP3P

For more information

For questions regarding this document or to engage CIPS for further consultation please contact:

Mary Jean Kucerak
Chief Operating Officer
905-602-1370 Ext 1
1-877-ASK-CIPS (275-2477)
info@cips.ca