Our Purpose, Identity, and Perspective

A collection of resources that help to define our identity and to guide our action.

1. Our 'About Us' Blurb - Used on our website and in our published materials

The BC Freedom of Information and Privacy Association (FIPA) is a non-partisan, non-profit society that was established in 1991 to promote and defend freedom of information and privacy rights in Canada. Our goal is to empower citizens by increasing their access to information and their control over their own personal information. We serve a wide variety of individuals and organizations through programs of public education, public assistance, research, and law reform. We are one of very few public interest groups in Canada devoted solely to the advancement of freedom of information (FOI) and privacy rights.

2. Our Formal Purpose - Per s. 2 of our Bylaws:

The B.C. Freedom of Information and Privacy Association (BC FIPA) shall exist for the following purposes:

1) To advance and support the principle that access to public information held by or for governments is vital to the public interest in a free and democratic society.
2) To advance the principle that privacy of personal information is also necessary to maintain a free and democratic society.
3) To encourage that the principles expressed in (1) and (2) above be entrenched in law and in corporate policy, in order to:
    a) Foster citizen awareness of and participation in public decision-making, and
    b) Secure an optimum state of public accountability, on the part of government and corporations.
4) To act as a public research, policy, information and educational resource on issues of freedom and privacy of information, as well as other key information issues.
5) To foster public awareness, promote co-operation and help develop consensus on information policy among concerned individuals and groups, including government, business, the legal community, academia, the news media, environmental groups, and other interested groups.
6) To do everything incidental and necessary to promote and attain the forgoing purposes.
7) For the attainment of the above purposes, to collect or raise monies in any manner in accordance with the Societies Act, and to distribute from time to time in accordance with the Societies Act, monies in support of the above purposes, including distributing monies to organizations with similar purposes.

3. Principles, consistent with our Purpose, that will inform our research, advocacy, contributions to policy and law reform, and communications:

3.1 General Principles:

3.1.1 Importance of Information and Privacy Rights

Information and privacy rights are vital to the functioning of free and democratic societies. We consider these to be human rights.

Protecting and extending information and privacy rights requires an active civil society and an engaged public. History shows us that governments and corporations tend to embrace secrecy and privacy-intrusive practices as a matter of course.

3.1.2 Non-Partisan but Politically Engaged

FIPA is a non-partisan organization. We have no affiliation with and will show no bias in favour of any political group. We will never endorse a political party.

We will actively engage with public debates regarding information and privacy rights and 'speak truth to power' as needed. This will often require us to criticize and / or support certain proposals or actions. Such engagement will always be guided by our commitment to our purpose and principles.

3.1.3. Rejection of Zero-Sum Framing

- "Public servants won't be able to give full and frank advice if they are subject to scrutiny through FOI".
- "Privacy protections inhibit police and national security officials from carrying out important public safety functions"

These narratives present information and privacy rights in a sort of zero-sum relationship with other important public goods and policy objectives. This sets up a politics of 'trade-offs', where limitations to transparency and privacy are framed as justifiable in the pursuit of security.

We reject this framing and should seek to avoid legitimizing it. Information and privacy rights are vital to a free and democratic society, and they should not be abrogated in the pursuit of other ends.

3.1.3 Rejection of Fatalism and the Politics of Inevitability

- "Privacy is dead. It is inevitable that everything we do is and will be watched and recorded".
- "ATI/FOI systems are destined to be irrelevant. Governments will always find ways to circumvent them and keep secrets".

We acknowledge that there are broad and systemic forces (with deep historical roots) that function to erode information and privacy rights. We also recognize that we are, in many ways, living in a surveillance society (and, to use Bernard Harcourt's term, an 'expository society', in which we are enticed and induced to produce and share vast amounts of personal information). However, we reject fatalistic discourses that treat the

principle of privacy as anachronistic and destined to be swept aside by technological and social changes. Similarly, we reject the cynical perspective that regards all ATI/FOI mechanisms as doomed to fail. Our stance is that information and privacy rights are vital and worth fighting for. Meaningful progress is possible, and steps can and should be taken to prevent further encroachment. Fatalism should be countered with advocacy and public education. BC (and Canada) can and should become world leaders in the recognition, protection, and extension of information and privacy rights.

3.1.4 Ongoing Reform

Protecting and expanding information and privacy rights is an ongoing and open-ended process. Societies should constantly review and update mechanisms and processes in order to ensure that information and privacy rights are meaningful, comprehensive, and appropriate given the current technological and socio-historical context.

We believe that Information and privacy rights - and the mechanisms and processes connected to them - should realistically reflect the current information ecology. If governments work with / through private partners, information and privacy rights should reflect this. Information and privacy rights should not be subject to undue limitations or barriers associated with jurisdiction or sector, especially if governments and corporations transcend these barriers through their work.

3.1.5 Emphasis on Law

Information and privacy rights should be entrenched in law and policy. Where change is necessary, it should be a priority to reform the relevant legislation. Changes in policy and practice are important and necessary, but they are not substitutes for meaningful law reform.

We support and encourage proactive efforts by governments and corporations to demonstrate transparency and openness, and to protect personal information and privacy. Proactive measures (ex. open government commitments) are not substitutes for strong transparency and privacy provisions enshrined in law.

3.1.6 Individual Responsibility

We want individuals to understand their information and privacy rights, and we want them to be empowered to make informed decisions regarding their personal information and their information rights. However, responsibility for protecting information and privacy rights should not be 'downloaded' onto individuals. Law and policy should require governments and corporations to observe clear and enforceable rules that protect information and privacy rights. Where there is evidence of structural gaps or shortcomings, the individuals should not be held responsible for plugging these gaps.

3.1.7 Accessibility

Information and privacy rights should be as accessible as possible. Systems should be designed to allow users to exercise the right to know and to exercise control over their personal information. Barriers - fees, delays, system complexity, etc. - function to inhibit information and privacy rights.

3.2 Principles Regarding Freedom of Information / Access to Information:

3.2.1 Right to Know Principles

We support and endorse the ten principles outlined on 28 September 2005 by the Open Society Justice Initiative [https://www.oas.org/dil/access_to_information_human_Policy_Recommendations_10_Principles_on_the_Right_to_Know.pdf]:

1. Access to information is a right of everyone.

Anyone may request information, regardless of nationality or profession. There should be no citizenship requirements and no need to justify why the information is being sought.

2. Access is the rule – secrecy is the exception!

All information held by government bodies is public in principle. Information can be withheld only for a narrow set of legitimate reasons set forth in international law and also codified in national law.

3. The right applies to all public bodies

The public has a right to receive information in the possession of any institution funded by the public and private bodies performing public functions, such as water and electricity providers.

4. Making requests should be simple, speedy, and free.

Making a request should be simple. The only requirements should be to supply a name, address and description of the information sought. Requestors should be able to file requests in writing or orally. Information should be provided immediately or within a short timeframe. The cost should not be greater than the reproduction of documents.

5. Officials have a duty to assist requestors

Public officials should assist requestors in making their requests. If a request is submitted to the wrong public body, officials should transfer the request to the appropriate body.

6. Refusals must be justified.

Governments may only withhold information from public access if disclosure would cause demonstrable harm to legitimate interests, such as national security or privacy. These exceptions must be clearly and specifically defined by law. Any refusal must clearly state the reasons for withholding the information.

7. The public interest takes precedence over secrecy.

Information must be released when the public interest outweighs any harm in releasing it. There is a strong

presumption that information about threats to the environment, health, or human rights, and information revealing corruption, should be released, given the high public interest in such information.

8. Everyone has the right to appeal an adverse decision.

All requestors have the right to a prompt and effective judicial review of a public body's refusal or failure to disclose information.

9. Public bodies should proactively publish core information.

Every public body should make readily available information about its functions and responsibilities, without need for a request. This information should be current, clear, and in plain language.

10. The right should be guaranteed by an independent body.

An independent agency, such as an ombudsperson or commissioner, should be established to review refusals, promote awareness, and advance the right to access information.

3.2.2 Duties to Document and Retain

Governments must be required to document certain activities and decisions by creating records that incorporate adequate and accurate details. A meaningful duty to document must be enshrined in law. Public bodies must also be required to preserve records according to clear policies. The systematic creation and retention of records is a prerequisite to the functioning of the legal right to know.

3.2.3 Timeliness

We believe that 'access delayed is access denied'. The centrality of the right to know to the functioning of a free and democratic society means that delays can impact both government accountability and the ability of individuals to participate in the democratic process. Requests should be processed in a timely fashion, and extensions should be justified and subject to statutory time limits and independent review. Systemic delays should not be tolerated.

3.2.4 Minimal Limitations

There should be no 'black holes' in our information laws. Government rights to withhold certain information should be limited and subject to a public interest override.

3.2.5 Resourcing

Governments must ensure that the offices responsible for facilitating and protecting the right to know (including Commissioners) are adequately resourced. Further, these offices require the resources and support necessary to fulfil the letter and spirit of applicable FOI laws. Backlogs, systemic delays, high turnover, and burnout should not be the norm within ATI/FOI units.

3.2.6 Operational Independence

Government offices and employees responsible for the processing of

information requests should be free from political interference.

3.2.7 Independent Review

Requesters should be able to request independent (Commissioner) review of all adverse FOI decisions. Commissioners should be empowered to review all records relevant to a given file, without any categorical exemptions. Commissioners should have order-making powers.

3.3 Principles Regarding Privacy

3.3.1 Foundational Principles for Privacy Protection

We support and endorse the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofperso naldata.htm

These guidelines include eight principles:

Collection Limitation Principle

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the *Purpose Specification Principle* except:

1. with the consent of the data subject; or
2. by the authority of law.

Security Safeguards Principle

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as

the identity and usual residence of the data controller.

Individual Participation Principle

An individual should have the right:

1. to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
2. to have communicated to him, data relating to him within a reasonable time;
    1. at a charge, if any, that is not excessive;
    2. in a reasonable manner; and
    3. in a form that is readily intelligible to him;
3. to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
4. to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

A data controller should be accountable for complying with measures which give effect to the principles stated above.

3.3.2 Meaningful consent

In the privacy realm, individuals are routinely asked to consent to the collection, retention, storage, and use of their personal information.

Consent is often treated as a way of circumventing laws and regulations that would otherwise prohibit certain uses of personal information.

We believe that meaningful consent must be free (voluntary), informed, and ongoing. Individuals must have both the right and the means to withdraw consent (as it pertains to the collection and use of their personal information) at any time.

We believe that consent can only be legitimate if it is not coerced. In practice, this must mean that there are meaningful alternatives available to individuals who do not choose to consent to privacy-impacting practices.

3.3.3 Surveillance

We recognize that current law, based on data protection principles, does not protect individuals from surveillance by public and private actors. Surveillance comes in many forms, sometimes justified for security reasons and sometimes implemented as an accessory to a convenience or service an individual has 'consented 'to. Surveillance includes CCTV in public, data collection as part of an individual's use of mapping or 'smart 'services and products, and analysis of an individual's behaviour for marketing or intelligence gathering.

We believe that surveillance, both overt and covert, undermines civil rights that are guaranteed by the *Charter of Rights and Freedoms*. By subjecting citizens to

constant watching and data collection, individuals must second-guess their actions, inhibiting among other things the freedoms of association, assembly, religion and belief, expression and thus creativity, and broader participation in political space.

We believe that the harm of surveillance is not mitigated by conventional “take it or leave it” mechanisms of consent, nor are the harms remedied by merely restricting access to data or by anonymization of data. The very act of surveillance undermines the freedoms that are fundamental in a free and democratic society.

We expect public and private actors to provide a high standard of justification for the use of surveillance related to law-enforcement. We expect actors to conduct surveillance only as a last resort.

We expect providers of ‘smart ’services and products to provide these with full functionality without requiring consent to surveillance as a precondition.