

October 1, 2020

Manager of Access and Privacy Strategy and Policy Unit
Ministry of Government and Consumer Services
Enterprise Recordkeeping, Access and Privacy Branch
134 Ian Macdonald Blvd.
Toronto, Ontario
M7A 2C5
(Submitted via email to access.privacy@ontario.ca)

Dear Manager,

RE: 20-MGCS015 Public Consultation - Reforming Privacy in Ontario's Private Sector

The Ontario Federation of Agriculture (OFA) is the largest general farm organization in Ontario, proudly representing more than 38,000 farm family members across the province. OFA has a strong voice for our members and the agri-food industry on issues, legislation and regulations governed by all levels of government. We are passionate and dedicated to ensuring the agri-food sector and our rural communities are included, consulted and considered in any new and changing legislation that impacts the sustainability and growth of our farm businesses.

Ontario's diverse and innovative agri-food sector is a powerhouse for the province – growing and producing more than 200 farm and food products, fuelling our rural communities and driving the provincial economy by generating more than 860,000 jobs and contributing over \$47 billion to Ontario's annual GDP. We are the leading agricultural advocate for Ontario farmers, their businesses and their communities.

OFA fully supports ensuring the privacy of our members' personal information. We believe their personal information should be protected and not released without their consent by anyone, including the government. We applaud the Ontario government's intention to address gaps in Ontario's legislative privacy framework and to establish comprehensive, up-to-date rules that will protect privacy rights. These government reforms are long overdue.

Although the ministry's "Privacy Reform Discussion Paper" does not define personal information, we consider name, physical location of personal residence, address, contact information, as well as any other information that could be used to identify name, physical location of personal residence, address or contact information, to be the most sensitive personal information. It is the case with many farmers, as with some other business owners, that their personal information is the same as their information for their business. Therefore, any release of this business information consequently results in release of their personal information. In these cases, we believe the business information should be afforded the same protections and privacy considerations provided to personal information.

There are many reasons why personal information should be kept secure and its use and/or release strictly controlled. Ontarians should rightly be concerned about illegal uses of their personal information, such as identity theft and other fraudulent activities. Farmers and their families face even greater risks to their personal safety and security. Farm families caring for livestock may be identified and targeted by militant animal rights groups. Other farm families may also suffer similar threats to their lives and livelihoods from those against certain farming methods and those intending to disrupt our food supply. As noted by the Rand Corporation: “Unfortunately, the agricultural and food industries are vulnerable to disruption, and the capabilities that terrorists would need for such an attack are not considerable.”¹ The World Health Organization confirms this vulnerability, stating “Agricultural production areas can be vulnerable to deliberate contamination...Irrigation water can be easily contaminated with chemical and biological agents”. The risk to fruits and vegetables is enhanced given that these products are often consumed directly, without processing and therefore more susceptible to contamination being undetected². These concerns are not unfounded in Ontario. Ontario farmers have experienced water pump equipment being vandalized and have also had people impersonating provincial officials attempting to gain access to their property. Incidences on livestock farms have also been reported.

The Discussion Paper makes note that current provincial laws (Freedom of Information and Protection of Privacy Act (FIPPA), Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), and Personal Health Information Protection Act (PHIPA)) govern the collection, use and disclosure of personal information by government and specific health care providers. Regrettably, we find current provincial laws wholly inadequate in the protection of sensitive personal information when that information is also business information.

In response to a recent FIPPA application, the Ontario Ministry of Agriculture, Food and Rural Affairs (OMAFRA) advised of their intention to release Farm Business Registration details even though many farmers have explicitly advised OMAFRA that they do not consent to such a release of their information. Clearly Ontarians should have more control over their own data held by government.

OFA strongly recommends that the FIPPA be amended to ensure information is not released by government without the consent of the person(s) the information relates to, and that business information be treated as personal information when the business and personal information are the same information, or the business information could be used to obtain the personal information of the business owner(s) or employee(s).

OFA has grave concerns regarding some information currently available online as part of Ontario’s Open Data Directive. Some datasets can be used to identify the personal information of Ontario farmers through their farm business information.

OFA has requested the Ontario Ministry of Environment, Conservation and Parks (MECP) remove Permits to Take Water (PTTW) application information from the data it makes available through the Open Data initiative. MECP currently releases information including the location – with GPS/UTM locations pinpointing exact water source locations on a map, permitted water volumes, intended water use (i.e. agricultural), and the name and address of the permit holder and the permitted amount of water allowed to be taken.

¹ Peter Chalk. Agroterrorism: What Is the Threat and What Can Be Done About It? Rand Corporation. 2004.

² World Health Organization. Public health response to biological and chemical weapons: WHO guidance, 2nd edition. Geneva. 2004.

As another example, the Workplace Safety and Insurance Board (WSIB) website's open data catalogue includes "Business Classification Details". This dataset contains a list of businesses with their Predominant Class for that year as of April 30 of the prior year including the business' Legal Name, Address, Predominant Class and NAICS Predominant Class Description. A sole proprietor's name and address released through this dataset would most likely also be the personal name and personal address of the sole proprietor.

OFA strongly recommends that the Ontario government remove and cease to make available through Ontario's Open Data, or any other initiative, all business information which may identify, or may be used to identify, personal information.

As noted in the Discussion Paper, Ontario does not currently have regulations for privacy in the private sector and relies on the federal Personal Information Protection and Electronic Documents Act (PIPEDA). We also note that the private sector must also abide by Canada's Anti-Spam Legislation (CASL).

OFA is in favour of expanding the scope and application of personal information privacy regulations to include non-commercial organizations, including not-for-profits, charities, trade unions and political parties, in addition to commercial organizations. However, it is important that any new privacy laws are not frustrated by other Ontario legal requirements placed on commercial and non-commercial organizations.

OFA recommends amending provisions in the Ontario Corporations Act and the Ontario Not-for-Profit Corporations Act that require the release of shareholder/member contact information to third parties to instead require a corporation, when appropriate, to send the information directly to its shareholders/members on behalf of the third party.

OFA employs this best practice when it distributes candidate information to voting members on behalf of an OFA member seeking a Director or Officer position in an upcoming OFA election. This ensures OFA remains in control of its member's contact information.

Another best practice employed by OFA is having our privacy policy available to all members as well as users of our website. OFA's privacy policy explains our practices with respect to personal information. It states OFA's commitment to privacy; OFA's responsibilities for all personal information under its control; the purposes for which personal information is collected, used, and/or disclosed at or before the time of collection; and that OFA will obtain the consent of the individual to the collection, use and/or disclosure of personal information except in limited circumstances, as permitted or required by law. In the policy, OFA agrees to limit the amount and type of personal information collected to that which is necessary for our identified purposes; to limit the use, disclosure and retention of personal information; to use our best efforts to ensure information is accurate, complete and up-to-date; and to protect the personal information with appropriate safeguards. Upon request, OFA's Privacy Officer will inform an individual of the existence, use and disclosure of their personal information and in most cases give the individual access to their personal information. OFA's Privacy Officer is also empowered to respond and to any complaints including, if necessary, amending our policies and practices.

Therefore, OFA fully supports the proposal to increase transparency for individuals by:

1. providing them with more detail about how their information is being used by businesses and organizations;
2. having clear consent provisions allowing individuals to revoke consent at any time, and adopting an "opt-in" model for secondary uses of their information; and
3. giving individuals the right to obtain their data in a standard and portable digital format.

With respect to the right for individuals to request information related to them be deleted or deindexed, i.e. “the right to be forgotten”, we believe this right should be subject to certain limitations such as when the information is required by law (for example the requirement to have a contact list of all members/shareholders of the corporation) or when complete information is needed for an emergency response purpose (such as a foreign animal disease outbreak).

The Discussion Paper also speaks to introducing requirements and opportunities to use data that has been deidentified and derived from personal information, to provide clarity of applicability of privacy protections. OFA cautions that data derived from personal information which has been deidentified can sometimes be reidentified by merging the data with other datasets. Therefore, it is critical that a new made-in-Ontario privacy law consider the risk of how likely information in deidentified data might be reidentified.

OFA appreciates the opportunity to provide written comments on the proposed privacy reforms. We also appreciated the invitation to participate at the September 9th agricultural sector consultation regarding this initiative. We would be more than happy participate in further discussions on these important reforms.

Sincerely,

A handwritten signature in black ink, appearing to read 'Keith Currie', written in a cursive style.

Keith Currie
President

cc: Honourable Lisa M. Thompson, Minister of Government and Consumer Services
Honourable Ernie Hardeman, Minister of Agriculture, Food & Rural Affairs
OFA Board of Directors