M E M O R A N D U M

April 15, 2021

To: ULC Drafting Committee on Personal Data Protection Act

From: Stephen Y. Chow

Re: Draft for April 23, 2021 Meeting

As in the new title, "data" that is protected is "data in a record." This is in accord with the Fair Information Practices Principles (FIPPs) that is not directed to traditional "privacy" or "autonomy," but to the "privacy" (limitation of use), security and integrity of records collected about data subjects.

These FIPPs are not directed to the security, integrity, access, correction or deletion of "information" held in the minds of people. Some "information" in the minds of people may be protected under the Uniform Trade Secrets Act. Under the HIPAA Privacy Rule, "information" includes spoken information, which is protected in the context of healthcare, but regulation here restricting, accessing, correcting or information spoken or thought would conflict with the First Amendment, even if it were practicable.

What is protected is certain information about a data subject that is recorded, that is, data about a data subject. Some formulations of protected information include the information that establishes that other information "about" a data subject is actually identified to that data subject. We include the information about a data subject and an "identifier" in "personal data" ("direct identifier") and "pseudonymized data" (other than "direct identifier", but suggesting that there was a process of pseudonymization rather than correlation of person-proxies). However, unlike the "flat filing" (fixed field in a single "line" of record – which provided the "identifier" link for actual identification of a data subject to the data about the data subject) that was the model for FIPPs, later relational data bases and today's on-the-fly correlation of data sets rely on the data structure or inferred patterns (dynamic algorithms) which might not be in a record at all.

I was comfortable with the March draft division of "personal data", "pseudonymized data" and "deidentified data" because it didn't subject to individual data subject access, correction and deletion to the kinds of data sets used in "machine learning" to find patterns. Regulation of those data sets should be considered with better understanding than the stakeholders in our project.

I understand that the new framework of "maintaining" partly meets my concerns on access, correction and deletion. However, **section 5(b) should clarify that it only applies to personal data subject to section 5(a)** (pseudonymized data maintained [along?} with [or including?] sensitive data). The redundant statement of "personal data or pseudonymized data" in section 7(c) should be removed.

To avoid ambiguity, we should stick with the definition (4) of "data" as "information in a record," in line with the ALI and actual practice without clear conflict with the First Amendment. Indeed, definition of (9) "maintain" also implicate the "record" aspect of "personal data" in a "system of records" – in line with the original FIPPs.

A **proposed change** to make this more consistent:

> Section 2(11): "Personal data" means ~~information~~ data that identifies or describes a particular data subject by a direct identifier or is pseudonymized data. The term does not include deidentified data.

Thus personal data is a subset of data and is a superset of pseudonymized data and independent of deidentified data.

The usage of “information” in (7) “direct identifier” may be acceptable as specific information that may be separate from the particular data about a data subject such as a folder name. Its use in (16) “publicly available information” is appropriate to include, for example, non-record information “observable from a public location.”

I have a problem with section 11(b)(3)-(4) relative to the GLBA, since the “privacy” provision actually allows sharing with affiliated entities and sharing with non-affiliated entities with an annual notice and opt-out. There is no regulation of access, correction or deletion and no further regulation for data shared under GLBA. **At very minimum, section 11(b)(4) should be restricted to data actually shared by the financial institution, which might be held accountable by its regulating agency**, not just data that “is subject to” GLBA such as financial information of customers, whatever the source. Call it “personal data” according to this Act. The actual term in GLBA is “Non-Public Personal Information.”