Privacy In 2021: Developments You Should Watch Out For



All indications are that the evolution of privacy laws and their impact will continue to evolve, perhaps even at a greater pace, in 2021. In celebrating Privacy Day, January 28, 2021, we would like to share four things businesses should be keeping their eyes on, and planning for, in 2021.

1. Significant changes to privacy legislation in Canada.

Canadian federal and provincial governments have tabled and proposed sweeping changes to privacy laws in Canada. For example:

- **Federal:** The federal Bill C-11, the *Digital Charter Implementation Act*, 2020, which proposes to introduce the *Consumer Privacy Protection Act* as a replacement for *PIPEDA*. The new legislation, if passed, will require businesses to adopt significantly more robust accountability measures such as a well documented privacy management program (not just a policy). It will also provide greater rights to individuals, and it includes significant order making powers and stronger enforcement measures in the form of fines and penalties.
- **Quebec**: Quebec has also introduced Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information*, which is intended to overhaul its provincial private sector privacy legislation. It, perhaps, gives a more significant "nod" to more modern laws, like Europe's GDPR, in its approach, including particularized individual rights and duties on organizations as well as the power for the Commission d'accès à l'information to impose significant administrative monetary penalties.
- **Ontario**: The Ontario government has released a discussion paper indicating its interest in enacting a provincial, private sector, privacy law (which are currently only in place in British Columbia, Alberta and Quebec but indications are could be quite different), something which the legislature has not previously succeeded in doing.
- **British Columbia:** British Columbia will be reviewing its *Personal Information Protection Act*, and the expectations are that this will include proposed revisions to add breach notification requirements and other changes to align it with other privacy laws.

2. The United States is getting into the Privacy Law game in a serious

way

The impact of privacy law developments in the United States on Canadian business cannot be understated. So many of our clients, customers, and service providers are based in or have ties to the U.S.

California has pushed the agenda with the emergence of consumer privacy protection and rights laws through ballot initiatives. The *California Consumer Privacy Act* and the *California Privacy Rights Act* (*CPPA* and *CRPA*) have implemented a number of privacy "firsts" in the U.S., including a privacy focused regulator with full power to implement and enforce the privacy laws. In addition to narrow requirements regarding individual rights over consumer data and prohibitions on "selling" (defined broadly) that information without opt-in express consent, these laws provide for individual rights of access and correction, as well as to restrict usage. Special provisions are placed on geolocation information and sensitive information. Employee personal data will not be covered until 2023 and there will be expanded breach liability with a private right of action.

We anticipate other states will follow suit with similar legislative initiatives, and Congress may attempt to address an unwieldy patchwork of state legislation by bringing in federal privacy legislation.

3. Continued development and enforcement of GDPR

GDPR continues to reveal its implications as the European Data Protection Board provides guidance on various issues and implementation of the regulation, and the European Court of Justice interprets and applies the law.

Significant issues to be sorted out this year include:

- The status of Canada's adequacy standing under GDPR (it is widely anticipated that Canada's federal privacy laws continue to provide adequate protection to personal data).
- The U.S. was not determined to be an "adequate" jurisdiction but the EU-US Privacy Shield Framework was, until it was struck down by the European Court of Justice last year. Absent another solution, legal transfers of personal data from the EU to the US will remain very challenging.
- While the UK's data protection law and requirements mimic GDPR, implementation and compliance in the UK will have their own nuances and will not be seamless with the rest of Europe. The European Commission will also be determining the UK's adequacy for data transfers, which may create a significant barrier.

The remaining EU will likely see more effective and coordinated enforcement of GDPR under the European Data Protection Board, as well as valuable guidance outlining policies on AI, biometrics, profiling, cloud services and blockchain, with a focus on data security (i.e. privacy by design and default, accountability).

We anticipate there will be greater enforcement regarding cross-border transfers of personal data.

4. Operating system privacy "enhancements"

Whether the motivations are privacy as a principle, consumer confidence, regulatory compliance or otherwise, we already see greater movement by the developers of operating systems, particularly Apple iOS (and some Android variants), to highlight privacy features, such as greater transparency and control over use and sharing of personal information. For practical reasons, such as the desire to make applications

available on these operating systems, developers will want to address these features and requirements.

We expect that consumers will see more privacy options, opt-ins/outs and “nutrition” labels about how apps use and share data in 2021.

by Ryan Berger and Cory Sully
Lawson Lundell LLP