大成 DENTONS KENSINGTON SWAN

Doing more business with data means doing more work on privacy

APRIL 2020

Hayley Miller
Partner

Hayden Wilson
Partner

While terms such as 'social distancing', 'bubble', 'essential service', and 'self-isolation' may have quickly become part of your and your business' vernacular, as we move out of lockdown for the first time, many organisations will need to reflect and readjust their practices to better suit the brave new world.

From a privacy perspective, life after lockdown will almost certainly look a lot different: Organisations will collect and deal with more data than ever, both for the purposes of offering products and services in what's recently been coined the 'shut-in economy' and to provide measures to better protect personnel, clients, and end-customers from the spread of the virus.

Take contact tracing as an example: In the not so distant past, mass government surveillance of the public's movements would trigger Orwellian alarm bells. But the New Zealand Government's recent announcement that a technology-based solution will be introduced to help with contact tracing follows many calls for this exact type of approach.

Rapid access to granular information about individuals' movements will assist health officials to quickly contain and manage instances of COVID-19, once life begins to return to normal, in a way that simply can't be matched by the use of aggregated information or manual processes, and in a manner in which we have not seen before.

The post-lockdown world will present many challenges and opportunities for businesses, especially when it comes to data.

Globally, lockdown has facilitated the emergence of the 'shut-in economy', where on-demand is the new norm, which has already ushered in a range of new data-driven product and service offerings.

Increased consumer demands to access anything, at any time, from the safety of our homes will continue to drive a significant shift of focus from physical stores to e-commerce platforms and from in person experiences to remote solutions.

Closer to home, we have also seen many businesses adjust their product and service offerings to give them a higher chance of being deemed 'essential' as we move in and out of Level 4 of the COVID-19 Government alert system – cafes have become boutique grocery delivery services; restaurants are moving to 'heat and eat' meal services.

In addition to existing businesses adapting their offerings to suit the new normal, in the coming months and years we expect to see a paradigm shift in the way businesses operate, in a manner which would have seemed absurd mere months ago.

For instance, many organisations will face pressure from clients and the public to ensure their supply chains are demonstrably safe. This may lead to, for example, procurement processes requiring stakeholders to demonstrate that their personnel adhere to physical distancing requirements. In a similar vein, organisations may roll-out bespoke contact tracing application software which enables them to directly

collect granular and specific information about their personnel's movements. While being tracked by your employer to ensure you've not been infected by a virus seems absurd, this could well be the new reality.

Beyond contact tracing, we'll inevitably see an increased focus on technology-based solutions, pitched as helping to contain the spread of COVID-19. For instance, it may well become part of a normal night out to present a digital immunity verification card to gain entry to a restaurant or bar. Advertisements for 'internet-of-things' solutions such as smart-thermometers and smart-PPE may not cause us to even raise an eyebrow.

Underpinning most, if not all, of these changes will be data. And – particularly where individual's health is involved – very sensitive data.

The upshot is that developing the tools, products, and services to best respond to a post-lockdown world must be accompanied by transparent, user-centric privacy practices. For many, responding quickly to consumer needs and Government rules and regulations will mean compliance falls to the wayside.

The biggest challenge for many will not be immediately apparent but will come further down the track: that is, trying to do business while dealing with the fallout of relying on a piecemeal, ad-hoc privacy framework to process personal information.

Failing to be transparent about your collection and use of information will raise alarm bells for consumers and regulators alike, and could damage the reputation of your business. Prior to the pandemic, consumers (and regulators) were becoming increasingly anxious about the overcollection of personal information – especially where this occurred on the basis of long, complex, impenetrable privacy statements.

While privacy laws are often criticised as a 'hand brake' on innovation and progress, this is undeserved.

New Zealand's principles-based approach to privacy regulation is neither dogmatic nor prohibitive. This means that not only are New Zealand privacy laws receptive to innovation generally, they are also flexible in allowing for personal information to be collected and used, within reason, where there is a real need.

The best way to mitigate the risk of privacy concerns 'stifling' innovation is to design a product, service or solution in a user-centric manner, from the outset. If the user's interests are kept at the heart of the design process, the end product will almost certainly align with the key privacy concepts of transparency and fairness.

Even if you are confident that your existing privacy practices are compliant, the changing face of data in a post-lockdown world will almost certainly require businesses to reassess and readjust their practices.

In particular, establishing a clear framework for collecting and processing information might include grappling with the following considerations:

- **What will we be collecting and why?** First and foremost, a privacy-centric model means understanding, articulating, and sticking to a clear purpose for collecting information. Chances are that untangling your key purposes may not be as straightforward as you anticipated. But identifying them at the outset will be crucial to ensuring you can use and process that information as anticipated.
- **How will we respond to changing consumer expectations?** As we adjust to the new normal, consumer expectation will shift. While 'mass surveillance' will be seen by many as essential for our response to COVID-19, the values and calculations underpinning this attitude will shift. And businesses should be prepared to adjust their practices too.
- **Does our pandemic response need a sunset clause?** The speed of the spread of COVID-19 – as well as the global and national response – should not be taken to mean that permanency is appropriate. In fact, creating frameworks that anticipate and allow for changes in the way data will be collected will be essential for ensuring business continuity. Establishing clear expectations that your collection and use of highly sensitive information should cease when it is no longer absolutely necessary will better equip your business to keep pace with the response.
- **Do we really need this information?** While the potential of 'big data' can be alluring, especially when it comes to products and services aimed at containing COVID-19, at a practical level, the more personal information collected by an agency, the greater the cost of storage – both in terms of server space and risk of a data breach. Is collecting voluminous amounts of information worth this risk in the long-run?
- **How will we know when the information can be shared and who it can be shared with?** Who will make decisions about how data you are responsible

for is processed? Will it ever be appropriate to pass on your employee's health information – even when deidentified – to a potential client? What will you do if the Government asks for information you've collected?

- **Are our existing security safeguards appropriate?** You'll need to determine whether your current data storage solution will be inappropriate in the circumstances, especially if you're relying on external vendors to develop digital solutions on your behalf. It is essential that you have clear and detailed discussions with vendors about how those solutions will collect and use information, including information that might be collected incidentally. In the end, the reputational risk of over-collection, inappropriate collection, or disclosure comes back to your organisation.
- **Are we being fair?** If one of your purposes for collecting information is to determine who is 'high risk' and who isn't – for instance, in the context of establishing persons in your workforce that should remain at home – how will you make those decisions? While it may be tempting to rely on algorithmic enhanced decision-making to sort through the swathes of data you may collect, this carries a risk of unfair discrimination – and is a strategy that isn't likely to be viewed kindly by the regulator.

Key contacts

Hayley Miller
Partner
D +64 9 915 3366
M +64 21 870 477
E hayley.miller@dentons.com

Hayden Wilson
Partner
D +64 4 915 0782
M +64 21 342 947
hayden.wilson@dentons.com

Click to revisit The Big Reset Hub