

Regulating for Globalization

Trade, Labor and EU Law Perspectives

Australia looks to decryption of communications and competition reform in the operation of digital platforms

Andrew Hudson (Rigby Cooke Lawyers) · Tuesday, February 26th, 2019



For a variety of reasons Australians have wholeheartedly embraced the various means of electronic communication and social media platforms.

One lawyer's brief history of the digital revolution

In large part, technological progress has been benign, albeit confusing for certain generations. After all, when I first started in the law, our most sophisticated form of communication was by telex. International phone calls were a complicated and expensive process and social engagement was largely limited to family and geographical proximity. I had to get approval from management for the use of “post it notes” and my fellow articulated clerks looked on enviously as I was the first of us to be allowed to have a speaker phone in my office.

The changes to practice have been significant and in large part beneficial even if it has meant that there are many more demands both for products and time of delivery.

I should add at the outset that I am by no means an expert on technology so I will confine myself, so far as possible, to some of the legislative and policy developments which have arisen due to concerns on developments

Revolution isn't without concerns

The speed of development with digital technologies often outstrips the pace of regulation which can even make regulation redundant. That situation can be made worse when the communication of technologies move across borders. This has created a series of significant concerns which have led to legislative and other responses.

One of the most pressing of those concerns was over the increased use of encryption in electronic communications which meant that the law enforcement agencies could not read those communications increasing the risk of its use for illegal purposes including terrorist activities. There had been similar concerns over the ability to access a person's device where that person refused to provide a password or otherwise enable access.

One of the other pressing concerns related to the control of operation of the platforms and the ability to ensure that what is presented is both reasonable and accurate and that the platforms are conducted in a fair manner without handing over undue control to the larger corporations and other groups (such as governments). There have also been many claims of misuse of the data collected by the platforms.

Australia has now taken some dramatic steps in legislating access to encrypted communications and proposing regulation of popular electronic platforms

Securing access to encrypted communications

Australia moved early to introduce the *Telecommunications and Other Legislation (Assistance and Access) Act 2018 (Act)*. As you would expect at the time of its introduction, there were very differing views expressed on the need for the Act as well as its terms.

Many saw it as being potentially damaging to basic privacy rights or as counter-productive to the development of industry in Australia. That was met with responses that any adverse consequences were outweighed by larger safety and security concerns and the assertion that data was not safe anyway.

In an attempt to get the Act passed a number of agreed amendments were then passed but without full debate on the basis of promises that the terms of the amendments and the Act itself would be subject to a review, which is currently taking place. In the meantime the Act (including amendments) had received Royal Assent in December 2018.

In general terms, the Act allows Australian law – enforcement agencies to seek or compel access to encrypted communications or information. The Act aims to give those agencies access to information (especially end – to – end encrypted services), for which the company providing the service would not have the “keys” required to access the information. The ability to compel access is not confined to the Act but the Act creates a more extensive regime.

There has been significant interest on the Act not just in Australia but also overseas on the basis that whatever is undertaken to comply with directions from Australian authorities (for example by creating a “backdoor” even a complex one) may fatally compromise the security of the device (or devices). That could also allow access by authorities overseas as the providers are faced with orders for access to the Australian process. Government has responded by holding that it is not intended to create backdoors and is only intended to create a framework to provide access if needed with protection against being required to take steps that would allow for a “systematic weakness”. In this context, the Act is different to recent legislation in the UK which allows agencies to secure warrants to hack into computers without requiring the creation of “back doors” or other means for further access”.

The means to seek or compel access can be summarised into the following categories

- Technical assistance Notices which are compulsory notices for a communication provider to use an “interception capability” they already have
- Technical Capability Notices which are compulsory notices for a communication provider to build a new interception capability, so that they can meet Technical Assistance Notices
- Technical Assistance Requests which have been categorised as voluntary requests.

The issue and content of the Notices are closely regulated being subject to a number of threshold tests including identification of the types of crimes which allow for their issue. There has been widespread condemnation of the definition of “systematic weakness” which is seen as too vague to provide a legitimate defence against Requests or Notices. Business groups are also concerned that it is not clear when businesses will have to act. Submissions have highlighted that Australian developers and other individuals could face jail time if they are unable to comply with a Notice. The Law Council of Australia has also identified questions around the treatment of persons by law enforcement officers if they are the person who can help with decryption. It pointed out that there is no clarity on the time to provide assistance and the ability of persons to contact family or a lawyer before being required to provide assistance. It further pointed out that the requirement to attend a place and provide assistance could be seen as tantamount to detention of the person subject to the direction

There also seems to be a high degree of concern over the Technical Assistance Requests. Even though they are not compulsory and no penalties follow from a failure to comply, the content of the Request can be much broader than the Notices. In addition, the mere issue of a Request would create pressure on the recipient who may not want to be seen to adopt a position adverse to that of the relevant agency or of government by refusing the Request and could end up with the recipient delivering more information than it could be compelled to provide.

Submissions are still being taken on the legislation and the Joint Committee on Intelligence and Security is set to report by April 3.

While implementation of the Act is not yet clear there are some obvious concerns for those potentially affected by the Act who will now need to look at consequences including revising terms and conditions to warn users on possible compulsory Government access to the data on devices as well as how to respond to Requests or Notices. No doubt a number of businesses may also be considering their operations or other presence within Australia as well as training for their employees.

The Australian competition authority looks at the operations of “digital platforms”

The good news for those involved in the digital world in Australia did not end with the Act. On 10 December 2018, our federal competition authority, the Australian Competition & Consumer Commission (ACCC) released a preliminary report entitled “*the potential issues created by the concentration of market power and the broader impacts of digital platforms.*”

According to the associated media release from the ACCC it had reached the view that:

“Google has substantial market power in online search, search advertising and news referral and Facebook has substantial market power in markets for social media, display advertising and online news referral”

On that basis the ACCC is of the view that such power is reducing the value of other business media (including print media) which has lost revenue to digital platforms. The ACCC also expressed concerns over a perceived lack of transparency in Google and Facebook’s key algorithms and other factors which influence the order of items shown in Google searches and the types of stories appearing in the Facebook “news” feed.

While the conclusions may not be surprising, the important consequence is that the ACCC is now proposing to recommend action to regulate the monetisation of media business content and the extent to which consumers’ data is collected to provide for targeted advertising. It is also seeking additional information on the way in which both platforms operate and manage information as they potentially manipulate outcomes.

The report contains 11 preliminary recommendations and identifies 9 areas for further research. One focus is that further research on the types of disclosures made and information provided around the collection and use of data provided by customers be conducted. It is probably fair to say that while most users of the platforms appreciate that there is a degree of capture and use of data provided, the extent of that capture and use would be of real surprise. After all, who really reads all those terms and conditions in detail and appreciates exactly what is being done? Most consumers are predominantly concerned on the speed of access to the information being sought and do not appreciate the consequences of making their information available. Given these concerns, the ACCC is considering a further recommendation to make it easier for parties to delete their personal information from a digital platform. This would be consistent to the consumer data right (CDR) being introduced in Australia to give “consumers the right to safely access certain data about them held by businesses.” It would also allow direction of that information to trusted third parties.

Preliminary recommendations by the ACCC

As stated above the ACCC has released 9 preliminary recommendations which can be broken down into 5 main categories.

- One category are measures to address Google and Facebook’s market power. These include review of the competition effect of a merger on the amount and type of data which would be acquired through a merger, the need to provide prior notices of a proposed acquisition and the provision of consumer choice by compelling the offer of choice of browser and search engine rather than having a default setting

- The second category are measures to monitor the activities of digital platforms and the potential consequences for news media organisations and advertisers. The recommendations here include establishing a regulatory authority to monitor, investigate and report whether vertically integrated platforms meeting the revenue threshold are engaging in discriminatory conduct. Further, the recommendations include the authority to monitor, investigate and report the ranking of news and journalistic content by platforms and the provision of referral services to the new media businesses (subject to a threshold revenue limit).
- Measures to address regulatory imbalance include government conducting a separate independent review to design a regulatory framework to regulate the conduct of all activities performing comparable functions for the production and delivery of content in Australia.
- Measures to assist a more effective removal of copyright infringing material including the ACMA determining a mandatory standard for “take down” procedures.
- 4 recommendations have been provided to better inform consumers when dealing with digital platforms and to improve their bargaining power. This includes recommendations for better disclosure on and collections of personal information including better legislative protection in the event of serious invasions in privacy and more stringent conditions around the use and collection of personal information. This would also include a provision that unfair contract terms should be illegal as opposed to just voidable with civil financial penalties to apply for their use.

The areas for further analysis proposed by the ACCC

The ACCC also identified a number of other areas of interest but, due to the timings could not be included and the preliminary report and has included nine proposed areas for further analysis.

For these purposes, the ACCC is considering views from stakeholders on the following issues.

- Further consideration of measures to support choice and quality of news and journalism;
- Improving news literacy online through the development of a broad campaign targeted at improving Australians’ understanding of how news and journalism is curated and displayed on social media and other digital platforms;
- Improving the ability of news media businesses to fund the production of news and journalism;
- The creation of a digital platforms ombudsman;
- Monitoring the pricing of intermediary services supplied to advertisers or websites for the purpose of digital display advertising;
- Third party measurement of advertisements served on digital platforms;
- Further consideration of measures to enable consumers to delete user data held by digital platforms;
- Whether targeted advertising should require express, opt-in consent; and
- prohibition against unfair practices.

Further developments

Clearly, many of these preliminary recommendations and areas for further research could lead to significant changes in the way of operation of digital platforms. It is worth noting that the ACCC work is not the sole review of this area. For example, on 14 February 2019 a joint report was released by the Productivity Commissions of New Zealand and Australia entitled “Growing the digital economy in Australia and New Zealand – maximising opportunities for SMEs” The report also considers regulation in the digital economy provision of government services in the digital economy and the trans-Tasman economy. A number of similar issues are raised in that report.

The ACCC will issue a further report later in 2019.

To make sure you do not miss out on regular updates from the Kluwer Regulating for Globalization Blog, please subscribe [here](#).

This entry was posted on Tuesday, February 26th, 2019 at 6:18 am and is filed under [Australia](#). You can follow any responses to this entry through the [Comments \(RSS\)](#) feed. You can leave a response, or [trackback](#) from your own site.