National Security and the Internet of Things: Practical Considerations for M&A Counsel

By Elliot Greenstone & Mark Katz

Introduction

Technology has dominated M&A activity in recent years and the trend shows no signs of slowing. In Deloitte's most recent *State of the Deal* study, nearly one-in-five survey respondents stated that they would focus M&A activities on technology asset acquisitions in 2018.[1] And, indeed, as early as Q1 2018, reports documented over 500 discrete tech deals in the United States alone, representing over US$60 billion in value.[2] As the pace of tech M&A quickens, legal counsel and other M&A practitioners face a range of challenges – some familiar, others new.

One of these newer challenges, the foreign investment national security review, has sparked concern among M&A practitioners that proposed transactions may be prevented from closing if they appear to present a risk to public safety or national strategic interests. The proposed takeover of Qualcomm Inc. by Broadcom in early 2018 provided a stark example.[3] Governments in the United States and Canada have long pushed back against foreign control of defense technologies and critical infrastructure, but recent changes in the tech, telecom, and consumer electronics markets have carried some of these fears into areas that had previously flown under the regulatory radar. In particular, the emergence of the so-called Internet of Things ("IoT") has given life to a host of new security concerns which weigh heavily on the deal making process.

1 https://www2.deloitte.com/content/dam/Deloitte/us/Documents/mergers-acqisitions/us-mergers-acquisitions-2018-trends-report.pdf

2 https://www.businessinsider.com/biggest-tech-mergers-acquisitions-q1-2018-4/#7-sap-americas-24-billion-acquisition-of-calliduscloud-1

3 https://www.reuters.com/article/us-qualcomm-m-a-broadcom-merger/president-trump-halts-broadcom-takeover-of-qualcomm-idUSKCN1GO1Q4

This article offers a broad overview of the national security review processes in the United States and Canada, with a particular focus on the impact of the legislation in the IoT space. It presents the general process and timeline of a national security review and outlines some of the considerations that should guide counsel's approach to such a review, should it occur.

First and foremost, as in any transaction, counsel for both buyer and seller should familiarize themselves with the particularities of specific assets being transferred in order to recognize the potential cybersecurity risks that an acquisition may present.

Defining the Internet of Things

Broadly speaking, the IoT refers to the growing interconnection and interoperability of web-capable devices, appliances, objects, and vehicles. Embodied in the idea of "smart homes" and "smart cities", the IoT is remarkable for its dual ability to provide consumers with network-connected product ranges, such as the Google Home and Amazon Alexa, and to increase business' capacity to collect data on consumer habits and lifestyle choices. For instance, in early 2018, Amazon acquired the video-doorbell company Ring for approximately US$1 billion. On its face, the acquisition provided Amazon with a compelling product to add to its line of smart home appliances. However, it was not long before certain observers suggested that the acquisition could also permit Amazon to track parcel deliveries and reduce mail-order fraud by accessing, with permission, smart doorbell data.[4] Put simply, as the consumer gains access to an integrated product line, the company gains access to an integrated data set.

From a security perspective, the IoT blurs the line between "consumer tech" and "critical infrastructure." Governments are justifiably concerned about the creation of software "back doors" which could be used to grant access to foreign intelligence agencies and malicious actors. The collection and concentration of user data in the hands of IoT companies is bound to draw regulatory attention to acquisitions in that space.

Experienced M&A counsel will undoubtedly have gained familiarity with the due diligence and regulatory challenges associated with consumer data collection in recent years. Most corporate counsel will have in their toolkit a basic understanding of data protection, intellectual property, anti-spam legislation and cybersecurity. But as the number of high-profile national security interventions in the consumer tech space is expected to grow, it is fair to assume that legal counsel will be called upon to advise on the sensitive process of national security review, in some cases for the first time.

The first step, particularly from the acquirer's perspective, will be to engage local, specialized counsel. However, even before this decision can be made, it is necessary to know when a national security review may be triggered, and how it can be expected to unfold.

Committee on Foreign Investment in the United States - CFIUS

The primary regulatory entity responsible for national security review in the United States is the Committee on Foreign Investment in the United States ("CFIUS"). CFIUS is mandated to review any proposed or pending transaction which could result in control of a US business by a foreign person (a "covered transaction").[5] In the event that the review process uncovers a national security risk, CFIUS may recommend mitigation measures or, in more

4 https://www.zdnet.com/article/amazon-ring-acquisition-made-not-for-smart-homes-but-for-deliveries/

5 *The Foreign Investment and National Security Act* ("FINSA"), Public Law 110–49, 121 Stat. 246, amending section 721 of the *Defense Production Act* of 1950 ("DPA") (50 U.S.C. App. 2170).

serious cases, the suspension or cancellation of the transaction altogether.[6]

CFIUS review is voluntary, but non-participation carries the risk, albeit rarely applied, of forced retroactive divestment. In 2011, for example, CFIUS issued a friendly recommendation to Chinese telecom giant Huawei to unwind an already-completed acquisition of assets from 3Leaf or else face a formal order to divest.[7]

The Huawei episode provides a useful illustration of CFIUS' changing role in the regulatory environment. Despite the panel's traditional focus on defence procurement, critical infrastructure and US technological leadership, CFIUS has dedicated considerable energy to the mobile tech market. This role was strengthened when, on August 13, 2018, Congress adopted the *Foreign Investment Risk Review Modernization Act of 2018* ("FIRRMA"). In apparent recognition of the role of a changing cybersecurity environment, FIRRMA contains language highlighting the risks associated with transactions which:

- "expose, either directly or indirectly, personally identifiable information, genetic information, or other sensitive data of United States citizens;"[8] or
- create a risk of "exacerbating or creating new cybersecurity vulnerabilities in the United States or which are likely to result in a foreign government gaining a significant new capability to engage in malicious cyber-enabled activities against the United States."[9]

On this basis, it seems reasonable to assume that as IoT data collection capabilities improve, so too will the possibility that IoT acquisitions attract national security reviews.

THE PROCESS

A CFIUS filing formally begins with a voluntary notice of the proposed transaction. Notification initiates a 30-day review period. During this time, CFIUS may request additional information from the parties, which must be provided within 3 days. Failure to provide such information may constitute grounds to reject the voluntary notice.

In order to avoid repeated requests for information, CFIUS encourages parties to communicate informally prior to an initial notification. CFIUS permits parties to file draft notices or partial information sheets in order to ensure that a later filing will be as complete and accurate as possible. It is recommended that parties submit this draft notice at least 5 days before filing the formal notification. The submission of a draft notification permits counsel to inform themselves of the concerns that CFIUS may have with a proposed transaction and to prepare the relevant responses.

In roughly 40% of cases, CFIUS will decide to convert the review period into an "investigation" causing the total period to be extended by an additional 45 days.[10] An investigation will typically be warranted if:[11]

- CFIUS or a member of CFIUS believes that the transaction threatens to impair the national security of the United States and that threat has not been mitigated;
- An agency designated by the Department of the Treasury as a lead agency recommends and CFIUS concurs that an investigation be undertaken;

6 For a complete explanation see the *Regulation Pertaining to Mergers, Acquisitions, and Takeovers by Foreign Persons*, Office of Investment Security, Federal Register 31 CFR Part 800, Federal Register vol. 73, no. 226 at 70702 (the "Regulation")

7 https://www.reuters.com/article/us-huawei-3leaf/huawei-backs-away-from-3leaf-acquisition-idUSTRE71I38920110219

8 FIRRMA s. 1702(c)(5)

9 FIRRMA s. 1702(c)(6)

10 *CFIUS Annual Report to Congress for CY2015*, Department of the Treasury, released September 2017. https://www.treasury.gov/resourcecenter/international/foreigninvestment/Documents/Unclassified%20CFIUS%20Annual%20Report%20%20(report%20period%20CY%202015).pdf

11 See the *Office of Investment Security: Guidance Concerning the National Security Review Conducted by the Committee on Foreign Investment in the United States*, Department of the Treasury, Federal Register vol. 73, no. 236 at 74567.

- The transaction is a foreign government-controlled transaction; or
- The transaction would result in foreign control of any critical infrastructure of or within the United States, if CFIUS determines that the transaction could impair national security and that risk has not been mitigated

THE OUTCOME

In the event that either the review or the investigation uncovers national security risks, CFIUS is empowered to recommend or impose legally binding mitigation measures. In some cases, the mitigation measures imposed have involved written undertakings ensuring that only authorized persons are granted access to customer information, or that the foreign acquirer is prevented by firewall from having direct or remote access to the systems storing such information. CFIUS may even require companies to institute any manner of internal compliance mechanism, including the creation of a dedicated staff position.[12] Failing to develop appropriate mitigation measures, CFIUS may recommend the suspension or prohibition of the transaction.

In light of the above, there are often compelling reasons to file a voluntary CFIUS notice even in borderline cases. Neither the draft notification, nor the completed application constitute an admission that the transaction constitutes a covered transaction or that national security concerns are engaged.[13] CFIUS does not reveal that a notice has been filed, nor does it reveal any information disclosed in the course of a filing. More importantly, once CFIUS has completed its review, the transaction is granted "safe harbor" from any future security review. The fact of acquiring a certificate of "safe harbor" greatly reduces the need to allocate risk in a final purchase agreement, easing the overall uncertainties associated with the transaction.

12 *CFIUS Annual Report to Congress for CY2015, supra* note 10, at 21.

13 See the *Regulation*, *supra* note 6 at 70712.

Thus while national security review may present an additional hurdle, mechanisms exist to smooth the procedure.

Investment Canada Act: National Security Review

Until 2009, Canadian foreign investment review under the *Investment Canada Act* (the "ICA") was limited to determining whether the foreign acquisition of control of a Canadian business would be of "net benefit to Canada". This review process was (and is still today) primarily focused on the impact of the acquisition on the productivity and domestic and international competitiveness of the Canadian economy, with important considerations being how the transaction would affect the target business in terms of capital investments, R&D, employment, location of head office and participation of Canadians in management.

In 2009, the Canadian parliament amended the ICA by enacting a separate "national security review" process. Although some argued that the already existing "net benefit review" process was sufficiently broad to encompass national security considerations, the government considered that it was important to have a separate review process to assess these issues. The statutory test under this process is whether the proposed transaction "could be injurious to Canadian national security". If the government determines that a foreign investment would have this effect, it can prohibit the transaction from proceeding (or order that it be unwound if the transaction has already closed), order the divestiture of certain assets, or require any other conditions necessary to mitigate the identified national security concerns.

The ICA's national security review process differs from the net benefit review process in several important respects. First, the national security review process is not limited to acquisitions of control; it applies in the case of minority investments by foreign investors in Canadian businesses, as well as the establishment of "greenfield" businesses in

Canada. Second, there are no financial thresholds for review - even the smallest of investments in dollar terms can be caught; by contrast, depending on the circumstances, the net benefit review process may not be triggered unless the Canadian business has an enterprise value exceeding $1.5 billion. Third, there is no formal application process to obtain clearance; rather, the government is given a set time period within which it must decide whether to commence a national security review, after which the investor is entitled to defend its transaction. Finally, there is no definition in the ICA of what constitutes an injury to Canadian national security; indeed, one of the principal problems to date with the national security process has been a lack of transparency regarding the criteria used by the government to initiate reviews and order remedies.

The Canadian government has tried to address these complaints about lack of transparency by issuing both Guidelines on the national security review process and Annual Reports providing general statistics and observations. Importantly, the government has spelled out in more detail the types of issues it will investigate during its review, including whether the proposed acquisition is likely to give rise to concerns relating to (1) the potential for transfer of sensitive technology or know-how out of Canada, especially if the technology has military/security applications; (2) the potential to negatively impact critical infrastructure and the supply of critical services to Canadians or the Government; and (3) the potential to enable foreign surveillance or espionage.[14]

THE PROCESS

The national security review process is divided into several distinct stages. The initial trigger for the review process is the date upon which the government becomes aware of the transaction. Typically, this occurs when the investor makes its filing under the ICA's net benefit review process. The government then has 45 days to decide if it will (a) commence a formal review, (b) allow the transaction to proceed, or (c) take an additional 45 days to make its decision. In theory, if the government decides to proceed with a review, the process can take anywhere between 155 to 200 days to complete (depending on whether the government takes the additional 45 days to decide what to do). In practice, the government can extend the formal review beyond that, subject to the investor's consent.

THE OUTCOME

There have been at least 15 transactions subjected to a formal national security review since the process was enacted in 2009. Of those 15 transactions, four were blocked from proceeding; five were permitted to proceed on the basis of divestitures; four were permitted to proceed on the basis of conditions; and two resulted in the investor abandoning the transaction. Of note, it is evident that if a transaction goes to formal review, the result will be some sort of remedy, ranging from prohibition (compulsory or "voluntary") to proceeding only on the basis of conditions. Also of note is that many of these cases involved the communications space (wireless telecom, business communications, telecom components) As such, and as in the US, it seems reasonable to expect that these categories may soon grow to encompass an ever-widening range of IoT transactions.

As to what sort of conditions (short of divestiture) may be required, the government has recently provided a helpful summary of potential commitments (in light of the fact that actual settlements are not published). According to the government, investors may be required to agree to the following types of undertakings to mitigate national security concerns:

- Refraining from participating in projects or work relating to military or other sensitive activities as may be specified by the Government.

14 *Annual Report: Investment Canada Act 2016-2017*, Innovation, Science and Economic Development Canada (2017), https://www.ic.gc.ca/eic/site/ica-lic.nsf/eng/h_lk81126.html; *Guidelines on the National Security Review of Investments*, Innovation, Science and Economic Development Canada (2016), https://www.ic.gc.ca/eic/site/ica-lic.nsf/eng/lk81190.html

- Requiring Government approval of proposed business locations in order to avoid proximity to strategic assets.
- Notifying existing customers of pending new ownership.
- Requiring all servicing and support for some or all business lines to be conducted in Canada.
- Creating Government-approved corporate security protocols to safeguard information and access to a site, including firewalls and segregation of data and other systems with restricted access, background screening and security clearances for certain employees, requiring employee NDAs, and establishing restricted areas and other types of physical security enhancements.
- Requiring employee security briefings and attestation to compliance with approved security protocols.
- Implementing monitoring and compliance mechanisms, including records retention , production requirements and site inspections by either the Government or third-party compliance auditors, or both.

Practical Considerations for M&A Counsel

As national security reviews in both the United States and Canada expand to potentially target consumer tech and telecom acquisitions, M&A practitioners in the tech sector would do well to familiarize themselves with the national security review process. While such reviews remain infrequent, counsel should be aware of the triggers for national security review, and the steps to take to ensure a smooth process.

In the initial planning stages of a transaction, M&A counsel should remain alert to the factors that may attract regulatory attention:

a) Structure of the Transaction. Counsel should consider whether the transaction will have the effect of granting control of a domestic corporation or asset to a foreign corporation, either directly or indirectly, keeping in mind the broad scope of both the US and Canadian legislation. Small acquisitions, minority investments and corporate restructurings may trigger national security reviews if their ultimate effect generates concern. Counsel should also keep in mind the varying degrees of scrutiny that foreign ownership will attract depending on the geopolitical climate and the relationship between the acquirer's home country and the vendor's. In Canada, as in the U.S., Chinese investments tend to raise red flags. Other countries that have found themselves in the national security crosshairs in Canada include Russia and Iran.

b) Nature of the Business or Product. Consumer products in the IoT space are rapidly becoming a part of "critical infrastructure," storing large quantities of personal information and permitting access to broader networks. Counsel should inform themselves as to the technical specifications of the assets in question, their degree of network connectivity, and the risk (or the perceived risk) that the assets might permit the creation of software or hardware "back doors."

As a transaction progresses, and once it has been established that a national security review may become necessary, counsel may also wish to take the following additional steps.

a) National Security Due Diligence. Due diligence is an important opportunity to identify issues in corporate governance, intellectual property, financing, and data protection that risk being flagged as national security concerns. Many of these security concerns are best addressed by acquirer disclosure, or vendor due diligence on the acquirer. In conducting these reviews, counsel may wish to pay particular attention to the identity and personal history of the directors and officers of the acquirer, whose curriculum vitae will almost certainly be requested by regulators in the event of a national security review. Directors and officers who have served in foreign militaries and political

offices are particularly worthy of note. Depending on the country involved, the fact that the acquirer is a state-owned enterprise can be an obvious area of concern.

Counsel should also be encouraged to pay particular attention to the vendor's procurement and IT policies. A company that adopts a new network-connected technology, such as a smart doorbell or air conditioner, exposes itself to additional risk, not only of cybersecurity breaches but also of regulatory intervention to prevent such breaches from becoming national security concerns.

b) Informal Channels. Counsel for purchasers should consider using the informal channels provided by national security regulators in both the US and Canada to discuss potentially problematic transactions before signing. Indeed, in Canada, the responsible regulators actively encourage contacts and discussions as soon as is possible. These informal channels serve to identify potential concerns and also inform purchasers about the kinds of information that may eventually be required of them. In worst case scenarios, such informal contacts can be critical elements in deciding whether the purchaser should attempt to proceed with the transaction at all. In Canada, we are aware of at least one instance in which informal discussions persuaded a purchaser to abandon a transaction at the conceptual stage because t it had no reasonable chance of successfully bringing the transaction to completion.

All of these considerations must be appreciated in context, and in light of the particularities of each review process. National security reviews are still only affect a very small minority of transactions and no two iterations are alike. Each is a discrete exercise in risk identification and mitigation. M&A counsel must be equipped to identify latent risks, and to develop mitigation measures so that the national security review process does not bring undue delays or lead to ultimate failure.

Special thanks to Alec Angle for his assistance in the drafting of this paper.

For more information, please contact:

Elliot Greenstone

514.841.6581
egreenstone@dwpv.com

Mark Katz

416.863.5578
mkatz@dwpv.com