REFLECTION

Selected conversations from a study tour of Berlin and Brussels

Professor Lyria Bennett Moses, Director Allens Innovations Hub, University of New South Wales Sydney

August 2019

About the Author

Lyria is Director of the Allens Hub for Technology, Law and Innovation and a Professor in the Faculty of Law at UNSW Sydney. Lyria's research explores issues around the relationship between technology and law, including the types of legal issues that arise as technology changes, how these issues are addressed in Australia and other jurisdictions, and the problems of treating "technology" as an object of regulation. Recently, she has been working on legal issues associated with the use of "artificial intelligence" technologies, the appropriate legal framework for enhancing cyber security and oversight for law enforcement intelligence. Lyria is a member of the editorial boards for Technology and Regulation, Law, Technology and Humans and Law in Context.

The KAS-sponsored visit of a delegation of Australians to Berlin and Brussels in 2019 provided an opportunity to consider different responses to mutual challenges posed by cyber threats. These ranged from the role of data protection law, to the inclusion of high-risk vendors in new 5G networks, to the form of law and the European regulatory focus on cyber security. While the full richness of the conversations cannot be captured here, some highlights are summarised below.

There is some difference between how the relationship between cyber security and data protection laws is perceived in Germany and Australia. In Germany, these are treated as distinct legal and policy domains – the former concerns critical infrastructure and technical protections and the latter protection of personal data. In Australia, the two issues are often intertwined in policy debates. In particular, moving to a stronger data protection regime is more often linked with enhanced protection from cyber fraud and reduced cyber risk.

In Germany, the primary form of data protection is the GDPR, which is becoming more popular over time, in particular due to its ability to enhance trust online. There was some discussion around what Australia can learn from this, given there is no real mechanism in Australia for holding even large listed companies to account for data breaches, given the impact on share price is minor. While the GDPR is often viewed fondly in Australia, there remain issues in Germany. There are still some residual concerns about impact on innovation. Further, there are federal issues with different agencies are responsible for regulating the use of data – meaning one can have 16 decisions for the same violation (from each German state). Germany is currently looking to harmonise but it is challenging as the state agencies do not report to the federal government. Federalism also poses challenges for data privacy law in Australia, with different privacy laws in each state and territory in addition to the federal Privacy Act.

In regards to 5G and so-called high risk vendors, the Australian stance is that this was a risk-based decision rather than a trade-based decision or a decision about a particular vendor. The balance of risk is perceived differently in Germany as the focus of its relationship with China has been primarily economic. As a result, the German regulations will operate at a general level, requiring enterprises to demonstrate that they have not been influenced. This may lead to a similar result, namely the exclusion of some Chinese companies, but this will depend on how the general regulations operate in practice. The current question is whether there can be a more open framework at the network periphery than what may be required in the core – a question on which there are different views. The Australian view is that such a distinction is not possible in the context of 5G.

> **The Australian and US approach to the question of Huawei and 5G has forced the EU to think more deeply, but there remains difference of opinion concerning the relative balance of commercial and national security considerations.**

It is possible that Huawei would be able to litigate in Germany, or retaliate against German exporters, were it excluded from the 5G network. There is also significant work being done in Germany across ministries to better understand the current position in terms of foreign policy vis a vis China and the Pacific (internationally and within Europe), China's likelihood of interference, and technical questions about 5G and potential impact at different ends of the network. Generally, Germany is seeking to work with China and encourage it to engage constructively and in light of important values in the international sphere. It is also focussed on remaining a liberal open economy. Australia's perception of risk is different due to high Chinese ownership and geographical proximity. Both countries are concerned about theft of intellectual property and trade secrets in areas such as quantum computing.

From an Australian perspective, what stands out is the relevance of trust in a corporation (through finances and corporate structure) when it can be directed by its government. Ultimately, Germany's relationship with China is different to Australia's relationship, giving each a different perspective on the risks presented by Huawei. Germany is particularly conscious of freedom of trade and refuses to arbitrarily exclude vendors. Australia is more conscious of China's global ambitions. The major challenge is not espionage (that can be solved through end to end encryption, although the security agencies have other concerns about this approach) but rather sabotage of the network.

Germany is co-operating within the EU on a broader framework, which will involve certification and risk assessment. It is likely that the EU will differentiate requirements according to layers of the network; rural/urban divides do not work for Germany because there are state capitals of varying size. The European Network and Information Security Agency (ENISA) will also be involved and will propose a tool box of measures. This will hopefully lead to a level of harmonisation in the EU, but, because public security is not part of the EU agreements, countries can still make diverse decisions on national security grounds.

The world is currently dependent on very few suppliers with the goal of building local capacity in core technologies impracticable given the fast pace of development. This forces a choice.

The Australian and US approach to the question of Huawei and 5G has forced the EU to think more deeply, but there remains difference of opinion concerning the relative balance of commercial and national security considerations. In Europe, the telecommunications framework has a competition focus, which means operators compete to reduce costs. This makes using Huawei attractive.

Europe in general, and Germany in particular, have legislation focusing specifically on cyber security. In the EU, this has gone into effect and there is ongoing work on the framework for the development of national cyber security schemes, with different countries at different stages of developing these. The European law applies to all member states as of 28 June, also making ENISA permanent. ENISA aims to build cyber security capacity in member states and enhance awareness through initiatives like Cyber Security Month. It participates in a broader policy network and supports member states in event of wide scale cyber attack. EU legislation also creates an EU framework for certification of cyber security devices and products. Market players can get certificate from any EU state; that certificate is then valid for the whole EU. The legislation ultimately is about certification – depending on context, this is only sometimes mandatory and industry will be involved in the mandatory elements. At the moment many of the concepts are at a high level, eg "internet connected products" which covers hackable toys, data protection principles, fraud, etc. Member states have different views on these laws eg France is looking at a more interventionalist stance than Germany. The discussion in the UK remains more industry-friendly.

Germany also has cyber security legislation. This deals with critical infrastructure, including power, water, nutrition/food, IT and telecommunications. For these sectors, it is mandatory to file reports to the security agencies and government should there be any cyber threat events. The agencies can then collect information and support companies that have been attacked. The Act also established a Federal Office for IT Security, supported by a research institute that reports to the Federal Ministry of the Interior. That facilitates the collection of information and development of expertise.

There are maps being developed, by BDI working with Deloitte, of cyber security laws around the world. Interestingly, Australia was shown as not having any laws specifically dealing with cyber security. Partly, this is a definitional question. For example, Germany's laws deal with liaison between government and industry around the protection of critical infrastructure against cyber security threats, whereas Australia's laws on a similar subject matter are wider in scope (covering all security threats). There seems to be little benefit in mapping only countries that have laws that deal separately rather than holistically with cyber security threats. In particular, by suggesting Australia has no cyber security laws, users of the map may be misled in their understanding on which countries were using law to help manage cyber security threats.

Copyright

Editor

Katja Theodorakis

Publisher

Konrad Adenauer Stiftung (Australia) Limited
Regional Programme Australia and the Pacific

11/3 Sydney Avenue
Barton, ACT 2600
Australia

Tel: +61 2 6154 9322

www.kas.de/australia

Disclaimer

All rights reserved. No part of this publication may be reprinted or reproduced or utilised in any form or by any electronic, mechanical or other means, now known or hereafter invented, including photocopyng or recording, or in any information storage or retrieval system, without permission from the publisher.

The opinions expressed in this publication rests exclusively with the authors and their interpretations do not necessarily reflect the views or the policy of the Konrad Adenauer Stiftung.

Design, Layout and Typeset

Swell Design Group

Paper

100%
FSC
www.fsc.org
RECYCLED
Paper made from
recycled material
FSC® C102086

ecoStar+ is an environmentally responsible paper. The fibre source is FSC Recycled certified. ecoStar+ is manufactured from 100% post consumer recycled paper in a process chlorine free environment under the ISO 14001 environmental management system.