THE HONG KONG NATIONAL SECURITY LAW AND UK ACADEMIC FREEDOM

A REPORT COMMISSIONED BY THE BRITISH ASSOCIATION FOR CHINESE STUDIES

Dr Samantha Hoffman
July 2021

Author

Dr Samantha Hoffman has authored this paper in her capacity as an independent consultant. Her work focuses on the domestic and global implications of the Chinese Communist Party's approach to state security. Her research offers new ways of thinking about understanding and responding to China's pursuit of artificial intelligence and big data-enabled capabilities to augment political and social control.

Acknowledgements

Disclosures

The report findings reflect the author's views alone. They are not reflective of any institution with which they are affiliated, and the project was conducted in their capacity as an independent consultant.

The British Association for Chinese Studies (BACS) commissioned this report. Although BACS acted as an intermediary by forwarding occasional anecdotal material, or names of concerned parties who wished to speak with the author's research team, all research and analysis were conducted independently of BACS.

Cover Image

Adapted from image purchased with standard license from Shutterstock.com/ User Blablo101.

TABLE OF CONTENTS

1. INTRODUCTION

The British Association for Chinese Studies (BACS) commissioned an in-depth, evidence-based report on the impact of the Hong Kong National Security Law[1] and broader political currents in an age of increased online teaching on the UK Higher Education sector.

The study was conducted in the first half of 2021, beginning after the first term of teaching in the 2020-2021 academic year. The research is intended to provide the UK higher education sector with a robust understanding of the impact of these afore-mentioned developments (many of which pre-date the NSL) on classrooms, student supervision, teaching delivery and research.

The objective was to identify common themes and trends and offer suggestions that will help provide the basis for an evolving and constructive conversation among UK China specialists and help ensure the safety of all students and staff.

Recommendations are offered in the final section of the report, which are targeted at academics and universities, but also call for some government actions. The recommendations are directed at supporting the development of common approaches to navigate the difficult terrain the current situation creates for the field.

1.1 METHODOLOGY

BACS commissioned an independent report on issues related to the impact of the Hong Kong National Security Law, and the effect of the worsening political environment in the PRC on teaching and research. BACS asked for numerous sub-topics and themes to be addressed, covering issues ranging from self-censorship to the security of online teaching environments.

Over 25 individuals were interviewed for this report. The interviewees were all UK-based, and their work is either focused on China or they hold relevant roles across university management or the higher education sector. Academics and university staff in all stages of their careers, at various ranks, and from a wide diversity of universities across the UK were selected. Interview candidates who would represent diverse viewpoints and experiences were selected.

Due to the relatively small pool of potential interviewees, and therefore the higher likelihood that interviewees could still be easily identified (even if quoted anonymously), the decision was taken not to discuss the details of specific anecdotes directly, and to keep them intentionally vague so as not to reveal sources. Individual interviews were kept off the record, and no direct quotes are included.

A fully anonymised roundtable and separate interviews with UK-based students from Hong Kong was conducted because it was important to also compare their experience to what

---

[1] The term "Hong Kong National Security Law" is used for stylistic consistency. The author, however, believes that "state security" is the most accurate way to refer to the Chinese party-state's "national security" concept and "national security" laws. The state security concept has distinct characteristics. It is important to avoid mirror-imaging the PRC's concept of state security with the concept of national security that is commonly understood in liberal democracies. See:
https://www.congress.gov/116/meeting/house/109462/witnesses/HHRG-116-IG00-Wstate-HoffmanS-20190516.pdf

academics described related to the impact of the Hong Kong National Security Law on their teaching.

Finally, desk research was conducted before and after the interview stage. Based on this, some unsuccessful freedom of information requests were submitted.

1.2 KEY FINDINGS

1) **Among the UK-based career academics interviewed, a majority expressed concern about the prospect of – and some described facing – professional reprisals for speaking out on sensitive China-related issues.** These risks were understood to emerge from the Chinese government and from within their university. The Chinese government could restrict in-country access or even arbitrarily detain staff or students and impose sanctions. University employers (including departmental line managers) could impede career advancement or otherwise professionally undermine outspoken staff members. Those who worked on objectively less politically sensitive subjects tended to express a more inflated threat perception than those who worked on more politically sensitive topics.

2) **In response to questions on self-censorship following the enactment of the Hong Kong National Security Law, no interviewee said they self-censored. More than half, however, went on to describe anecdotes of either self-censorship or being censored. Many of these examples pre-dated the Hong Kong National Security Law.** There was no evidence or suggestion that course content had been altered in response to the law's passage. Examples of self-censorship included everything from decisions not to publish potentially controversial articles to avoiding making statements on traditional and social media that might be viewed as too critical of the Chinese state. Examples of being censored included being nudged not to express particular views critical of the Chinese state in traditional and social media and having PhD applicants rejected because their proposed thesis might be too politically sensitive.

3) **Although academics in China Studies fields were aware of the risks their courses could create for mainland PRC and Hong Kong-based students and themselves, this awareness did not appear to extend widely to those working on areas outside the field or university management.** Those involved in advising university-wide decisions understood institutional security risks that the Chinese government creates but still lacked a sophisticated understanding of China's security laws and their implications. In other cases, though, the problem was not ignorance but a clear choice by university management to overlook security problems for other reasons. Most evidence suggested this is either for financial gain or to avoid upsetting the Chinese government. This lack of awareness and minimal involvement of area specialists in security-related university governance appears to undermine risk mitigation approaches.

4) **Interviewees described a handful of cases of harassment of either themselves or, more commonly, that they had been made aware of cases of harassment toward their students from the mainland PRC or Hong Kong.** If reported officially, little to no action had taken place to protect victims, enforce university codes of conduct, or guarantee academic freedom and freedom of speech.

5) **University leadership and sometimes academic departments are not transparent about decisions that affect academics who work on China-related issues. This problem impacts both individual capacity and academic departments' ability to deliver safe learning environments.** Transparency issues are apparent across multiple areas, including decisions to procure technology from China-based technology companies or to engage in research partnerships. Relatedly, there were many complaints about inadequate accommodation of academics' voices in due diligence processes.

6) **Across interviewees, most expressed concern about surveillance and cybersecurity risks, but few, if any, seemed to have practical knowledge about how best to manage these risks.** Many academics took measures to reduce the risk for mainland PRC and Hong Kong-based students in online teaching environments but expressed a wish for more specific guidance on guaranteeing that their measures would enable and protect students.

7) **Solutions for providing China-based students access to UK university digital learning environments do not effectively mitigate the risks emerging from the Chinese government's policies.** Service providers and university IT departments appear to approach the procurement of solutions for overseas access to digital learning environments as a technical problem and do not properly assess the political risk. Part of the problem is that digital supply chain security is not adequately defined in current public policy debate, and this problem trickles down to university IT decisions.

8) **Interviewees expressed concern that existing avenues for communication and reporting problems to their university management and/or to government bodies were not accessible or responsive.** Although many interviewees wanted the government to take a more active role, they did not know how to frame the appropriate response.

2. MANAGING RISK UNDER INTERNATIONALISATION

In the UK, the internationalisation of higher education has offered many opportunities for universities. But, with opportunity comes risk. Internationalisation has augmented or contributed to new security-related challenges. Left unmanaged, they undermine values higher education institutions are supposed to protect, namely academic freedom.

An October 2020 Universities UK (UUK) report, 'Managing Risks in Internationalisation: Security Related Issues', touched on many of the issues interviewees raised in the research for this report.[2] The UUK consulted with academics in drafting the report, but ultimately the UUK represents vice-chancellors and not the specific interests of individual academics. University leadership is responsible for overseeing processes such as due diligence related to research partnerships and IP protection; they are responsible for protecting all university members (including students and staff); they are responsible for campuses' physical and virtual security. Day-to-day responsibility for reacting to this declining security environment in teaching and research, as it relates to China, still largely devolves to individual academics.

To date, efforts in the UK higher education sector to describe and manage the risks of internationalisation have not publicly and specifically addressed the impact of the political climate in the People's Republic of China (hereafter 'China' or 'PRC'). Nor have they contended with the way the downward spiral of China's bilateral relationships, combined with the July 2020 enactment of the Hong Kong National Security Law, have intensified threat perceptions for those doing research and teaching on China. The UUK report, for example, did not directly mention state actors. It was a missed opportunity to clearly and publicly evaluate the unique challenges different illiberal regimes can pose to the higher education system.

There was no evidence that the higher education sector has seriously evaluated its relationships with Chinese entities. This is despite there being ample evidence that among other illiberal state actors, the Chinese government represents an outsized risk to the higher education sector relative to other illiberal state actors. Politicians and research groups have been critical of the higher education sector's closeness to Chinese government-linked interests. But the sector itself has failed to directly and publicly identify the Chinese government or Chinese Communist Party as specific risk actors. There was no explanation for this failure other than, as several academics highlighted, the suggestion that University management usually prioritises the financial incentive of maintaining the status quo in their relationships with China.

As observed by one academic, these decisions do not uphold the values the the UK higher education system claims to uphold. Numerous UK universities, for example, have relationships with Fudan University.[3] Many of these relationships appear to continue undeterred even though Fudan University removed references to "academic independence" and "freedom of thought" from its charter.[4]

- The London School of Economics runs a double master's degree program with Fudan University, including an MSc in International Social and Public Policy[5], an MSc in

---

[2] https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2020/managing-risks-in-internationalisation.pdf
[3] https://archive.vn/1sAxT
[4] https://www.universityworldnews.com/post.php?story=20200110071137628
[5] https://www.lse.ac.uk/study-at-lse/Graduate/degree-programmes-2021/LSE-Fudan-Double-Masters-ISPP

Financial Statistics and Chinese Economy [6] , and an MSc in Global Media and Communications[7], among others. LSE also runs Summer Language Programmes[8] with Fudan.

- The University of Nottingham's Confucius Institute describes Fudan University as a "partner"[9]. The University of Edinburgh's Confucius Institute[10] is also partnered[11] to Fudan University.

- King's College London has had several international academic collaborations with Fudan University. King's has run a summer school with Fudan University[12]. In 2017 the King's Department of History formed a partnership with the university[13]. The Department of Digital Humanities said it has an academic collaboration with Fudan University[14].

Academics described students (from Hong Kong and mainland China) who approached them seeking guarantees that the university was attempting to guarantee their safety—such as opportunities to anonymise electronic submission of coursework, or opportunities to speak more freely in one-to-one meetings instead of in front of other students who they might not personally know and therefore trust. Rather than protection from being exposed to course content that could violate Chinese laws, UK-based students from Hong Kong wanted guarantees that the university would do everything in its power to protect them should they face harassment while studying and living in the UK.

Individuals who are critical of the Chinese government or who work on sensitive topics in their research or public commentary, felt vulnerable to state-driven discrimination. They did not trust that their university, if required, would offer necessary support. Interviewees described cases where academics were under increased China-sourced criticism for their stance on sensitive issues and simultaneously faced quiet admonition from their colleagues. In more than one case, this included serious attempts to undermine their credibility and attempts to encourage them to leave the university. Others were asked to change their tone in media or social media commentary. These instances did not appear to increase after the Hong Kong National Security Law's passage. They were already occurring for several years.

It is also important to note that a few academics who were not vocally critical of China in their research or public commentary said they were intentionally more cautious of being publicly critical of China. They indicated that this decision made them feel exposed to being accused of being too 'pro-China' by more vocally critical colleagues. However, these academics did not describe being undermined in the same way as the more vocally critical academics. For example, they did not experience a loss of access or invitations to China. They did not report that their colleagues threatened them, and they did not report being asked to censor themselves.

---

[6] https://www.lse.ac.uk/study-at-lse/Graduate/degree-programmes-2021/LSE-Fudan-MSc-Financial-Statistics-Chinese-Economy
[7] https://www.lse.ac.uk/study-at-lse/Graduate/degree-programmes-2021/MSc-Global-Media-and-Communications-LSE-and-Fudan
[8] https://info.lse.ac.uk/staff/divisions/academic-partnerships/university-partners/fudan-university
[9] https://archive.vn/F99r2
[10] https://theboar.org/2020/11/leading-academic-university-break-china-ties/
[11] http://www.confuciusinstitute.ac.uk/about-us/people/
[12] https://archive.vn/HD1kI
[13] https://archive.vn/a9gIu
[14] https://archive.vn/RkHvj

2.1 THE HONG KONG NATIONAL SECURITY LAW

The Hong Kong National Security Law was enacted on 30 June 2020[15]. For Hong Kong, the passage of the law was a watershed event, eroding any illusion that the Chinese government would continue to adhere to "one country, two systems". Specifically, the law criminalises separatism, subversion, terrorism, and collusion in and support for any of those activities by anyone in the world no matter where they are located. The law's extraterritoriality is not theoretical. In its first year the law has already been cited in arrest warrants for pro-democracy activists including citizens and those granted asylum in the UK and US[16].

Interviewees in the China Studies field were dismayed by the law and concerned for their students' welfare. The law heightened concerns for the welfare of mainland China-based and Hong Kong-based students, and many described specific actions they had taken as individuals or collectively to mitigate the risks. Many academics also described increasing tension affecting their students from Hong Kong, and therefore their classrooms, since the Hong Kong protests began in 2019 against the proposed Extradition Law[17].

Nearly all academics said they would not allow the Hong Kong National Security Law to impact their teaching. Some acknowledged that the law would inevitably affect teaching, in terms of the management of student welfare. However, they had not yet experienced a noticeable impact on teaching. Most said they had not received any direction to change their course delivery because of the law. Based on the syllabi for China Studies modules some academics provided, covering the same module before and after the law's enactment, there was no evidence that course content changed. There was also no evidence that lecturers made choices to avoid teaching any topic because Beijing would consider it sensitive.

The impact was much greater as it related to academics' perceived security of their operating environment. Despite committing to not allowing the law to affect teaching, many acknowledged that the Hong Kong National Security Law would affect their ability to conduct research on China. The most common issue raised was potential risk to personal safety if they returned to China. There was clear angst among those who rely on access to China to maintain dialogue (especially on more sensitive subjects) or to continue research in China on subjects where fieldwork is most essential.

Some academics reported that students from Hong Kong had approached them with concerns for their welfare, but this took place both before and after the law's passage, starting at the height of protests in Hong Kong in 2019. Some academics passed these concerns on to university management, but said they had received a very limited response. In one case, for instance, the university sent a mass message to students reminding them of welfare services available, but failed to specifically address students from Hong Kong, who had reported they were being harassed by mainland Chinese students. Others voiced their concerns and felt they were engaging with university management meaningfully to develop a response.

Many interviewees described the ways in which they, their colleagues, or their departments, responded to the law. In these instances, departmental line-managers tended to focus on duty of care to students, taking a protection-based approach. There was no doubt that most of the

---

[15] https://archive.is/H9Yvw
[16] https://www.theguardian.com/world/2020/jul/31/china-hong-kong-security-law-american-citizen-exiles
[17] https://www.amnesty.org/en/latest/news/2019/09/hong-kong-protests-explained/

academics were genuine in their attempts to protect students, and were doing what they felt they had to do to in order to guarantee student and staff safety. Yet, most were not able to explain why specifically their choices were seen as solutions the problem (and not potentially creating more harm by reinforcing the law's effort to curtail freedom of expression).

- At one university, course convenors were asked to evaluate political risk of their courses. If too risky, those courses were not offered to students learning remotely while based in Hong Kong and mainland China (due to Covid-19). The students were told they could instead delay their studies and await return to the UK to take the courses from within the UK, or take courses that were less sensitive.

- Some universities discouraged the recording of lectures covering sensitive subjects, and prohibited recordings of classroom discussion of these topics. This measure was publicly reported on for both the School of Oriental and African Studies[18] and the University of Oxford[19].

- At Oxford, it was also publicly reported that students would submit and present work related to China anonymously, and that tutorials would be held on a one-to-one basis[20]. Some universities already anonymised these processes to a degree, but some academics expressed that they thought anonymising coursework would harm academic freedom more than it would help protect students from the Hong Kong National Security Law.

- Others were working on improving ways of assessing risk or raising awareness internally, but were cautious not to act too quickly. The most common reason was to avoid reacting too quickly and, in their view, thereby allowing the law to succeed in its objectives.

- Academics who did not work in the China field were concerned by the law more generally, but did not see it impacting their teaching as directly.

Another response type was to focus on expectations for student conduct. There were efforts to develop new rules or guidelines to remind students of the code of conduct they were expected to uphold.

- In one case, students were asked to sign binding conduct agreements prohibiting recording classroom sessions.

- Other academics were in conversations with university management and colleagues on improving student codes of conduct, and enforcing appropriate consequences should those regulations be violated.

A large number of universities had not taken similar steps, leaving individual academics to organise responses on their own.

Interviewees described several instances where students from Hong Kong reported to their lecturers that mainland China students had harassed them. Those mainland PRC students who

---

[18] https://www.thetimes.co.uk/article/wipe-references-to-china-to-protect-students-soas-lecturers-told-9bjwlwwvm
[19] https://www.theguardian.com/education/2020/sep/28/oxford-moves-to-protect-students-from-chinas-hong-kong-security-law
[20] https://www.theguardian.com/education/2020/sep/28/oxford-moves-to-protect-students-from-chinas-hong-kong-security-law

were allegedly responsible, however, faced minor or no consequences. Others described students, from both Hong Kong and mainland China, approaching them to express fear that they would be at greater risk of being reported by other students in class for sensitive things they might say in class. Nevertheless, it is worth noting that some students interviewed who were studying less-sensitive subjects expressed less fear. Academics who reported conversations like these to line managers or university management often found the process unhelpful, in part because it seemed the seriousness of the situation in Hong Kong was not well-enough understood.

One publicly reported incident took place in October 2019 at the University of Sheffield[21]. Hong Kong students were protesting in support of Hong Kong, and were harassed by Chinese students. Ian Williams, in his recent book *Every Breath You Take: China's New Tyranny[22]*, described how a Chinese student made a death threat against a Hong Kong student and threw a beer bottle at them, adding that (pg. 152):

> "The bottle-thrower, a twenty-five-year-old student studying at Sheffield University's international college, was cautioned by police and briefly suspended by the university, but the intimidation continued. Hong Kong student activists were photographed and videoed by Chinese students, the pictures published online. They faced online trolling and death threats against them and their families back in Hong Kong. One was forced to move apartments."

Research on this case for our report indicated that it was assumed or implied that the student was permanently expelled. However, it was confirmed that the expulsion was only a temporary suspension from the student's program of study.

The general consensus among interviewees was that the Hong Kong National Security Law codified many of the unwritten rules for doing research on China. But most problems academics described pre-dated the Hong Kong National Security Law. Indeed, while the Hong Kong National Security Law was a watershed event for Hong Kong, its text is also in line with the Chinese party-state's articulation of its state security concept (see Footnote 1 on national security and state security) under Xi Jinping.

Some interviewees highlighted that for those operating in UK academia, especially those with familial links in China or Chinese citizenship, there was a long-standing high risk. For those with strong links to China, being in a more open operating environment did not mean that they were not at risk while operating in the UK, as they may be subjected to unwanted approaches or reported for any action seen to be less than patriotic.

On the issue of self-censorship, we were told that before the Hong Kong National Security Law was enacted, some academics had not submitted completed papers for publication, or altered for publication versions of papers because of possible risks to Chinese co-authors. In one case this was because of the fear that a co-author who relied on Chinese government scholarships would then lose the scholarship. Some academics also said they were cautious commenting on social media on sensitive issues like Xinjiang, because of the risk of losing access. Others described framing research questions in ways that avoided directly confronting the most

---

[21] https://www.bbc.com/news/uk-england-south-yorkshire-49914304
[22] https://www.amazon.com/Every-Breath-You-Take-Tyranny/dp/1780277113

sensitive aspects of issues, such as avoiding words like "authoritarian" to describe the Chinese political system.

In terms of going to China, many academics said they would no longer take the risk, partly because it would also hurt their own family if something went wrong. Some said they would be very upset to one day lose access. They knew that this was a possibility and would continue to attempt their research undeterred. However, those engaged in more politically sensitive research on China were increasingly finding themselves locked out of China.

3. DIGITAL LEARNING ENVIRONMENTS UNDER COVID-19

The COVID-19 pandemic forced teaching online, and forced many students from overseas to remain in their home country. When the requirement for students to have remote access to their UK university courses grew, most universities focused on making sure students had the technical ability to obtain access to their courses. For students from China, this meant the ability to gain access to content that would otherwise be blocked by the Great Firewall, such as YouTube videos.

Efforts to provide access to digital learning environments for these students were not focused on finding a solution that holistically provided secure access to this content. For academics in the China field, this raised many concerns that digital learning solutions could put both them and their students in a more vulnerable position.

The initial solution that attracted media attention was a pilot project run by UK-based not-for-profit company Jisc, a digital solutions provider to UK higher education institutions. According to Jisc, it worked with Alibaba Cloud on a solution for staff and students based in China (and potentially rolled out to other countries)[23]. The solution would "improve the quality and performance of connectivity, and reliable access to course material and virtual learning environment (VLE) systems while not on campus."

The system used Alibaba's Cloud Enterprise Network (CEN), which Alibaba describes as a "hybrid and distributed global network" where it could be used to facilitate communication between Virtual Private Cloud (VPC) to VPC, or VPC to on-premises data centres (IDC). The CEN, according to Alibaba Cloud, connects over 60 Alibaba Cloud access points worldwide[24]. The CEN is said to improve the speed (low latency, or low delay, between a demand and response), reliability (service works as reliably as expected) and availability (availability of cloud services across any given period of time)[25].

According to Jisc, the University of Southampton, University of York, Queen Mary University of London and King's College London, were all involved in a no-cost one month trial of the project. Interviewees familiar with the pilots said the project did not reach a stage where security from risks emerging from China's political system were a serious consideration. The Jisc solution was too expensive, according to interviewees familiar with the matter, and universities were priced out of purchasing it.

---

[23] https://www.jisc.ac.uk/rd/projects/supporting-enhanced-access-to-online-education-in-china
[24] https://alibaba-cloud.medium.com/compare-and-connect-part-two-8a7dd95826dc
[25] https://alibaba-cloud.medium.com/compare-and-connect-part-two-8a7dd95826dc

Jisc's relationship with Alibaba continued, and Alibaba's Global Education Access Framework has superseded the CEN as a purportedly more affordable option for universities[26]. Though, it is not clear how the Global Education Access Framework is materially different. According to Jisc, its initial efforts were China-focused, but the Global Education Access Framework was broadened to include the rest of the world[27]. The University of Birmingham was one university that started using the global education access framework. According to Jisc, "the solution isn't about providing unfettered access to the internet, or a way to bypass China's firewalls, but about giving learners as much of a guarantee as possible that they will be able to access services they need for educational purposes"[28].

It appears that most universities (such as the University of Edinburgh[29], University of Dundee[30], the University of York[31], Lancaster University[32], the University of Sheffield[33], and University of Westminster[34]) all use a Alibaba-provided VPN using Fortinet Software. The VPNs are intended for PRC-based students and staff attempting to access their university's digital platforms. The VPNs route the users' internet traffic to an Alibaba Cloud server in London, which will then allow them to connect to University digital learning platforms to access course content. Several universities referred students not to the University IT department but instead to Alibaba's Dingtalk platform, should they require technical assistance[35].

While the VPNs raised clear concerns for academics who understood the extent of the Chinese government's surveillance activities, this did not necessarily mean there was a clear understanding about their legality and vulnerabilities. Some staff advised that the VPNs are illegal in China and therefore should not be offered or advised as a solution. A VPN can be used legally in China, but the provider must be approved by the Ministry of Industry and Information Technology[36]. This means that use of VPNs to evade surveillance is increasingly challenging, any use of an approved VPN will be heavily monitored. An approved service is Alibaba Cloud, which many universities in the UK and around the world use to enable Chinese students in China to gain access to digital learning environments and relevant content (such as Microsoft 365).

Just because the VPN is officially approved and does not put students at risk of violating laws on VPN use does not mean that it does not put them at legal risk. VPNs are not always secure[37]. Taken outside of the China-specific context, for instance, a 2015 study at Queen Mary University of London found that many VPN providers were vulnerable to 'IPv6 leakage', where "the leaked information ranged from the websites a user is accessing to the actual content of user communications, for example comments being posted on forums"[38]. This report's

[26] https://www.jisc.ac.uk/global-education-access-framework
[27] https://www.jisc.ac.uk/international
[28] https://www.jisc.ac.uk/blog/from-obstacle-to-opportunity-1-mar-2021
[29] https://www.ed.ac.uk/information-services/computing/desktop-personal/vpn/vpn-service-using-in-china
[30] https://www.dundee.ac.uk/guides/connect-china-forticlient-service
[31] https://www.york.ac.uk/it-services/services/china-connect/#tab-5
[32] https://answers.lancaster.ac.uk/display/ISS/Alibaba+Cloud+Accelerator+installation+and+help
[33] https://www.sheffield.ac.uk/it-services/university-connect-china
[34] https://medium.com/ussbriefs/internet-access-deal-allows-chinese-government-censorship-in-our-uk-university-virtual-classrooms-4040a77df25d
[35] https://www.york.ac.uk/it-services/services/china-connect/#tab-5
[36] https://law.asia/vpn-compliance-china/
[37] https://www.qmul.ac.uk/media/news/2015/se/most-internet-anonymity-software-leaks-users-details.html
[38] https://www.qmul.ac.uk/media/news/2015/se/most-internet-anonymity-software-leaks-users-details.html

author has independently verified that the Chinese government is capable of monitoring VPN traffic, and it should be assumed this capability is certain for any approved VPN.

But even if the VPN provided is technically secure, it does not mean it is safe for students to use. It was clear that academics understood this because they were concerned about PRC-based students accessing what they deemed to be sensitive course content. It was not clear that universities understood, or made any attempts to educate users about these risks. As part of the pilot Alibaba CEN project, Jisc said it carried out due diligence in terms of GDPR, Data Protection and information security compliance to Jisc's standards. But, the fact that Alibaba was chosen as a secure provider illustrates those current methods for doing due diligence on China-specific technology issues are not effective enough.

Alibaba may be a nominally private company, but like most if not all Chinese technology companies, Chinese Communist Party presence within the company's structure creates a direct pressure point[39]. Alibaba has nearly 200 party branches[40] and amid a period of intense scrutiny of company founder Jack Ma[41], the secretary of one of Alibaba's Party committees said "Alibaba should adhere to correct political directions and maintain political integrity"[42].

Alibaba Cloud's International Website Privacy Policy, which includes applicability to registered users of Alibaba Cloud products and services, states that the company will collect, retain, use and disclose personal data for purposes including[43]:

> "to comply with applicable law, legal process or lawful government request, or in respect of any claims or potential claims brought against us or our parent companies, shareholders, subsidiaries and affiliates; performing risk control, legal compliance and sanctions screening; and performing screening and checks for unlawful, fraudulent, deceptive or malicious activities."

The policy also states that Alibaba Cloud could transfer the collected data to a jurisdiction outside of the data subject's jurisdiction. Alibaba Cloud states "recipients of the data in these jurisdictions may be subject to data privacy laws less protective or not equivalent to those in your own jurisdiction". It is standard practice for global companies to "acknowledge in their privacy policies that user data may be transferred and governed by laws outside of their own jurisdiction"[44]. What changes the risk-level for data subjects are how laws governing data might affect them once their data is transferred.

All data Alibaba Cloud collects could be transferred to company servers anywhere, and used precisely for the kinds of state security cases that a law like the Hong Kong National Security Law specifies. China's recently enacted Data Security Law[45] further increases risk, because the law applies not just to domestic data-handling activities, but also to data-handling activity taking place "outside the territory of the PRC", if those activities are seen to "harm the state

---

[39] https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2021-05/Party-state-Activities_Mapping-Chinas-Tech-Giants_Thematic-Snapshot.pdf
[40] https://chinatechmap.aspi.org.au/#/company/alibaba
[41] https://www.bbc.com/news/uk
[42] https://archive.fo/Eq889
[43] https://archive.vn/Kke0t
[44] https://www.aspi.org.au/report/mapping-chinas-tech-giants-supply-chains-and-global-data-collection-ecosystem
[45] http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml

security, the public interest, or the lawful rights and interests of citizens and organisations of the PRC".

For this reason, it is essential for universities and service providers to conduct due diligence in a manner that addresses the wide scope of problems emerging from the PRC's political system, not just technical vulnerability to attack or functionality. And they should keep in mind that the data the Alibaba Cloud VPN helps to generate might be combined with other user data, such as data from or related to the device they are using, which could include more specific details about location and their real identity.

A final additional issue that was raised was that academics described being automatically censored on social media platform LinkedIn over content in their profile that was deemed to be restricted in China. Those academics were concerned that students who had been censored would be at risk in China. But the violation accusation is not made in a case-by-case decision-making process according to the available evidence. Instead, LinkedIn appears to be automatically identifying profiles to censor based on key word combinations. Therefore, it is highly doubtful that individuals are physically at a greater risk compared to any risk they already faced while operating in China. This is not the same, for instance, as the case around the anniversary of the Tiananmen massacre involving Zoom, in which the company complied with a request to follow Chinese "local law' and shut down an overseas event commemorating Tiananmen[46].

4. RECOMMENDATIONS

Academics are aware of the risks that working on China creates but appear to make reactive decisions rather than proactive choices to defend core liberal academic values. Universities and academics need to ask themselves, what are the core values universities are meant to protect? Academic freedom is undoubtedly one of those hard-fought for values, but entanglement with the Chinese government threatens to undermine it. With this core value in mind, this report recommends the following:

1. **Universities should offer risk warnings before students become university members, not when they enrol in a specific course.**

   When a student decides to enrol in a university, it should be made clear that they may be offered courses that cover topics that do not conform with their worldview. If they are international students, the course content may not necessarily be authorised in their home countries. Warnings offered at the beginning of individual courses may create more significant risks for international students from authoritarian regimes, because of politically sensitive content. It would further single out those who might wish to engage with the subject critically. It also reinforces censorship or encourages self-censorship, potentially doing more harm than good.

   Duty of care is not just protecting students; duty of care should also be about enabling them to obtain the education for which they have paid. A well-written course abstract should clearly indicate what content will be covered. Students can decide for

---

[46] https://www.chinafile.com/conversation/chinas-zoom-bomb

themselves whether or not risk exists for them. If they participate, though, they should expect to be judged against peers.

2. **Universities should have an enforceable code of conduct, and proportionate consequences for violations of the code of conduct.**

   If they do not already, university codes of conduct must in unequivocal language mandate that no intimidation or harassment of any student or staff member is ever acceptable. Codes of conduct should specify that this includes activity in which staff or students disclose any harmful information about another member of staff or student to a foreign government or party acting on behalf of a foreign government. For victims who are Chinese citizens, the potential consequences for them, their family and close contacts -- in the PRC or other illiberal regimes -- could be severe. In the PRC, consequences could include imprisonment or harassment if they return to the PRC, regular short-term detention of their family and close contacts, seizure of passports, and other coercive measures.

   Cases in some UK universities of the intimidation of international students from Hong Kong by international students from mainland China are an example of the kind of severe infraction that should be investigated and prosecuted to the fullest extent of the law. This level of intimidation should mandate a criminal investigation of the students responsible. If universities or academics are aware of this type of misconduct, they have a duty to report it to the police. If a student is charged and found guilty of a serious criminal offence, that student must be expelled immediately. (It is worth noting that even though it is outside the scope of this study, UK universities also need to make clear that Anti-Asian racism against people of East Asian appearance will not be tolerated.)

   If an instructor is made aware of bullying, harassment or intimidation in their classroom, it should be reported immediately to the relevant university department. Intimidation or threatening behaviour should be considered a zero-tolerance offence where a warning is not an acceptable outcome. In any case, where a threat has been made a member of staff or student, the matter should be reported to authorities for possible criminal investigation. The University is responsible for preserving all university records and paperwork on the matter and handing it to the police as evidence. If found guilty, it is possible that if that individual is not a UK citizen, under Home Office Immigration Rules, entry clearance or permission to reside in the UK could be cancelled[47].

3. **Clear channels for reporting intimidation and harassment to universities and law enforcement should be made available to students and staff.**

   Universities must clearly advertise these channels to all students and in multiple languages, including English and Chinese. They must also be accessible and be seen as safe avenues for reporting sensitive matters. Not all international students in the UK have high English language competence, despite English language requirements.

---

[47] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/947441/cancellation-of-entry-clearance-and-permission-v1.0ext.pdf

Universities must guarantee that all students clearly understand their rights and pathways for seeking assistance on any issue related to their health and welfare.

4. **Values in UK higher education, particularly academic freedom, must always be projected in response the problems the Chinese government creates. Responsibility sits with academics, University management, and also with the UK government.**

   Maintaining the space provided by academic freedom and associated freedoms of speech and association must always be incorporated into universities' responses. Over time, reactive responses aimed at protecting potential victims could undermine academic freedom. Although protection-first approaches may seem appropriate to the moment, such measures, if continued overtime, could have a stifling effect on university life. The Chinese government and Communist Party goals, enshrined in laws like the Hong Kong National Security Law or the National Security Law of the PRC, are to narrow the field of speech, ideas, and research into state-approved forms. Any responses that result in censorship, caution, or losses to critical analysis help Beijing achieve its goals, even when the intention is to provide immediate protection

5. **UK higher education institutions must become more transparent with academic staff and must not make it so difficult for staff to understand basic information about how decision-making processes take place.** The lack of transparency across universities is appalling, and the unwillingness to provide information when requested is, for lack of a better word, shameful. In one case, which this paper does not describe in specific detail due to sensitivities for the individuals concerned, an interviewee gave very specific details and timeline, and contents of specific emails. The interviewee requested that the information be obtained through an FOI process to avoid identifying the individuals who passed on that information. The response was not only a refusal to grant access to any requested content, but also based on the verifiable information, some of the claims that university made were entirely fallacious. The UK's Freedom of Information Act (FOIA) does not appear to be serving its vital transparency functions, and UK lawmakers should seek to hold hearings on the Act and improve its language.

6. **Finally, a government-led full review of University IT arrangements with PRC-based technology companies should take place across all UK higher education institutions**. In a recent report "Supply Chains and the Global Data Ecosystem" this report's author also advised that governments "recalibrate data security policy and privacy frameworks to account for the Chinese state's use of data to reinforce its political monopoly"[48]. Many big Chinese tech firms, including Alibaba Cloud, explicitly note that they will share data rather than protect it. It is clear that IT departments do not understand that technical assessments of a product's security, for risks such as malicious intrusion or general reliability testing do not address the risks emerging from a vendor's political circumstances. PRC-based companies operate within a legal system that puts them at a greater risk of being subjected to politicised demands of the Chinese party-state, which means that data collected through any PRC company is at risk of being accessed or used against the data subject for state security purposes.

---

[48] https://www.aspi.org.au/report/mapping-chinas-tech-giants-supply-chains-and-global-data-collection-ecosystem