LIMITING CHINESE NATIONAL SECURITY ESPIONAGE

RISKS OF INTERDEPENDENCE

The Federal Bureau of Investigation currently describes China’s intelligence activities as “the greatest long-term threat to our nation’s information.”267 The bureau has thousands of active counterintelligence cases relating to China and opens multiple new cases daily.268 Although Beijing’s theft of intellectual property and other economically valuable data remains the primary concern, Chinese national security espionage is also harmful. China’s intelligence agencies have stolen a significant volume of U.S. military secrets in recent years, including aircraft designs.269 They have penetrated U.S. political campaigns to gain insight into future American policymaking.270 And they have compromised America’s own espionage networks, reportedly helping to expose and disrupt U.S. intelligence activities in China—a top American collection priority—and elsewhere.271

Classified U.S. national security secrets are shielded by a robust system of technological, physical, and personnel controls. As a result, China often first seeks out sensitive unclassified data that it can later exploit to acquire classified information. In particular, U.S. officials assess that China assembles and analyzes large quantities of Americans’ personal information to identify potential targets for intelligence collection or other subterfuge. Some U.S. intelligence officials believe such techniques have enabled Beijing to quickly identify undercover personnel from the Central Intelligence Agency around the world and monitor or disrupt their activities.272 U.S. agencies also cite the risk that China could use sensitive medical, financial, or other personal information to blackmail or co-opt American officials.273
China's intelligence targeting of American officials has become a major justification for U.S. tech restrictions. After all, U.S.-China technological ties provide the Chinese government with additional opportunities to harvest Americans’ personal data (just as these ties may give Washington ways to collect on Chinese targets). Beijing could, for example, pressure a Chinese tech company to share its private data on American users. Chinese companies are legally required to comply with such requests, and according to U.S. intelligence officials, these companies already help to process bulk data in the possession of Chinese intelligence agencies. For example, U.S. officials have publicly alleged that Huawei “has the capability secretly to access sensitive and personal information in systems it maintains and sells,” and that “information from Huawei routers has ultimately ended up in hands that would appear to be the state.”

**RISKS AND LIMITATIONS OF DEFENSIVE MEASURES**

These risks provide some basis for limiting Chinese companies’ presence in U.S. information systems. However, restrictive measures may always not be very effective in thwarting Chinese theft of Americans’ personal data, for the simple reason that Beijing seems to prefer other ways of acquiring that data. When American officials describe China’s most successful and damaging bulk collection efforts to date, they usually point to the devastating hack of the U.S. Office of Personnel Management and the compromises of Marriott, Equifax, and Anthem. But these were all remote cyber operations; none apparently required any Chinese insider access to U.S. systems, companies, or supply chains.

In fact, sensitive personal information about Americans can be bought outright from U.S. or foreign data brokers. U.S. journalists have vividly demonstrated how easy it is to obtain geolocation and other data to identify and track prominent Americans. The U.S. military and Intelligence Community reportedly use similar techniques to track foreign targets, so there is every reason to believe that Beijing does the same. Then there is simple data scraping from the open internet, which is apparently one of Beijing’s most effective espionage techniques. According to U.S. prosecutors, China has successfully recruited multiple Americans to spy for Beijing based on information in these targets’ public LinkedIn profiles. William Evanina, then director of the National Counterintelligence and Security Center, said in 2019 that LinkedIn was China’s “ultimate playground for collection.” (Although LinkedIn announced last year that it would leave the Chinese market, that won’t stop Beijing from scouring Americans’ own LinkedIn pages.)

**China’s most successful known bulk collection efforts were all remote cyber operations. They required no insider access to U.S. systems, companies, or supply chains.**

(Although LinkedIn announced last year that it would leave the Chinese market, that won’t stop Beijing from scouring Americans’ own LinkedIn pages.) The major digital espionage
risks, then, stem from pervasive gaps in U.S. cybersecurity and data privacy law, policy, and implementation. Chinese tech companies’ presence in American markets and supply chains seems like a secondary threat at most.

Before instituting sweeping measures to deny China any access to Americans’ personal data on national security grounds, it is also worth considering targeted actions to protect the relatively few U.S. citizens with access to classified information. The government has significant influence over its own employees and contractors, enabling Washington to discourage or even bar them from using Chinese technologies deemed to be high-risk. For example, the U.S. military already bans TikTok from government-owned devices. The military has even “urged troops and their dependents to erase the app from personal phones”; if necessary, this could become a condition for maintaining a security clearance. Protecting undercover agents is a more complicated task. But U.S. spy agencies have already implemented new tradecraft and operational security innovations to offset China’s digital counterintelligence techniques—the kind of cat-and-mouse game that has occurred throughout the history of espionage.

**RECOMMENDED POLICIES AND PROCESSES**

“Personal data” is not a useful or controllable category. Instead, the U.S. Intelligence Community should work to identify those categories of personal data that would provide the greatest marginal benefits to Chinese spy agencies. Regulatory agencies would then consider technology restrictions aimed specifically at this data, while accepting higher levels of risk for other types of data.

The Intelligence Community analysis would need to consider China’s preexisting intelligence capabilities and its access to functionally equivalent personal data on Americans. It would also examine the U.S. government’s ability to detect and mitigate different kinds of personal data theft. If Washington can learn of certain Chinese data theft quickly and implement effective response plans (for example, by readjusting official travel patterns or refreshing the cover identities used by intelligence officers), that category of data may need less protection. Finally, the IC should consider the overall significance of the U.S. personnel described by the data, and the likely harm to U.S. national security from China’s improved ability to track, recruit, or disrupt these people. While all Americans’ personal data deserves fundamental protections, extra-stringent restrictions should have special justification—just as the IC generates costly cover identities for some intelligence officers and not others. For example, data on enlisted U.S. military members in

Regulators should protect the personal data with greatest marginal benefits to Chinese spy agencies, while accepting higher levels of risk for other types of data.
non-sensitive positions would certainly have some intelligence value to China, but it may not be critical enough to justify broad-based restrictions on China’s involvement in the U.S. tech sector.\textsuperscript{283}

Because U.S. government data is already controlled to varying degrees, the Intelligence Community would primarily look to identify sensitive but unclassified personal data held by companies and other private parties. For a useful benchmark of the sensitivity of privately held data, the IC could ask whether the data would be considered classified if owned by the U.S. government. For example, U.S. national security agencies maintain large caches of employee data in unclassified, internet-connected systems (like the Defense Travel System) that are inherently more vulnerable to Chinese hacking than classified systems.\textsuperscript{284} The existence of such systems suggests that Washington believes the practical benefits of internet connectivity can often outweigh the risks of Chinese espionage. This is a reasonable calculation. Regulators should not require private companies to take more onerous precautions than U.S. agencies themselves take for equivalent categories of government-held data.

\textbf{CASE STUDIES}

\textit{Genetic data.} Genetic information is an example of personal data that could warrant restrictive measures to prevent Chinese government access. In 2020, the Treasury Department issued new regulations empowering CFIUS to review covered transactions that involve “sensitive personal data” of more than 1 million individuals.\textsuperscript{285} The definition of sensitive personal data includes genetic data. Compared to other types of personal information, genetic data is less widely distributed and harder for Beijing to obtain. China could conceivably use genetic information to identify and physically track U.S. government officials—including undercover officers—as they move around the world.\textsuperscript{286} Because someone’s genetic information cannot be changed, a breach would have lifelong consequences and be difficult to remediate.\textsuperscript{287}

\textit{Geolocation data.} In other cases, the “sensitive personal data” regulation seems overly broad. Geolocation data is also considered sensitive under the Treasury rule. Yet because Americans’ geolocation data can be easily purchased from online data brokers, CFIUS screening probably cannot prevent China from acquiring such data. Meanwhile, the possibility of CFIUS review could cause substantial economic harm to U.S. businesses. There are entire industries, including the mobile app ecosystem, where relatively small American companies might have geolocation data on 1 million or more individuals. The potential need to file voluntary CFIUS notices, and the opaque and time-consuming nature of CFIUS review, could chill a great deal of investment activity while doing little to protect Americans from Chinese espionage.
The Grindr episode illustrates both the possibilities and limitations of U.S. efforts to stop Chinese companies from acquiring different kinds of personal data on Americans. In 2019, CFIUS forced a Chinese company to unwind its purchase of the dating app Grindr.\(^{288}\) Grindr has a large American user base, likely including many U.S. officials, who privately share information about their HIV status and sexual activities with the app. Such information has great value for Chinese intelligence targeters, will remain relevant to them for decades, and cannot be found in many other places online. The CFIUS action therefore made sense, because it blocked one of China’s clearest paths to acquiring a unique cache of personal data with clear national security value. On the other hand, the forced divestment probably did little to secure other types of personal data, such as geolocation. A 2021 Norwegian government report revealed that Grindr’s new American owners routinely share users’ “IP address, GPS location, age, and gender,” though not sexual or health information, “with a very large number of third parties.”\(^{289}\) It would be a trivial task for the Chinese government to get similar information from data brokers.

**Stayntouch.** Trump’s 2020 executive order on Stayntouch provides another cautionary case study. Circumventing the normal CFIUS process, Trump required a Chinese company to divest from Stayntouch, a cloud-based service that helps hotels manage their properties.\(^ {290}\) Stayntouch has access to data on hotel guests, and its software can even be used to access guest rooms. This likely raised the specter of China using Stayntouch software to gain historical or real-time knowledge of U.S. government officials’ travels, a clear counterintelligence threat. That said, Stayntouch is used by only 500 hotels worldwide; American officials might be able simply to avoid these hotels.\(^ {291}\) By comparison, Marriott alone has 7,642 properties.\(^ {292}\) Without aid of any insider access, Chinese hackers had persistent access to Marriott’s Starwood network for *four years* and stole data on *500 million guests*, including reservation and travel information as well as personal data such as passport numbers.\(^ {293}\)

The contrast between Stayntouch and Marriott shows the limits of CFIUS as a tool for protecting Americans’ personal data. While a small number of high-value data sources can be protected through China-focused restrictions like investment screening, most other kinds of personal data cannot feasibly be secured this way. Unfortunately, U.S. officials have not always made such distinctions. The Trump administration, in particular, often lumped all types of personal data together regardless of sensitivity, uniqueness, or controllability. Then secretary of state Mike Pompeo in 2020 described a “project of real scale” in which “we are now evaluating *each instance* where we believe that U.S. citizens’ data . . . crosses Chinese technology.”\(^ {294}\)

**App bans.** In Trump’s last days as president, he signed an executive order banning Alipay, WeChat Pay, and six other Chinese apps. Rather than point to specific kinds of data these apps collected from Americans, Trump described a generalized threat of “Chinese connected software applications” that can “[access] personal electronic devices such as smartphones, tablets, and computers”—in other words, nearly all Chinese software. And he cited, as a
favorable precedent, India’s recent ban of “more than 200 Chinese connected software applications throughout the country”—a blunderbuss barrage from New Delhi that seemed motivated more by a desire to retaliate for recent border skirmishes than by any careful, app-specific security review.295

Pompeo and Trump are no longer in office, and Biden has rescinded the app bans. But the fact that such bans were even attempted, and the limitless logic used to justify them, has already sent a chilling message to the global software industry. Meanwhile, loose talk about “Americans’ data” can still be heard across the political spectrum. Evanina, a former career professional, testified last year that approximately “80 percent of American adults have had all of their personal data stolen by the [Chinese Communist Party], and the other 20 percent most of their personal data”—a head-scratchingly vague and implausible claim that has nevertheless become widely quoted.296

**Video games.** Under Biden, CFIUS has reportedly continued its investigation of Tencent’s ownership stakes in Riot Games and Epic, two video game developers.297 A former civil servant in charge of CFIUS reviews under Obama and Trump explained these investigations to *Bloomberg*: “When you’re talking about massive amounts of data, there’s probably something for the committee to look at.” He went on to add that: “The question then becomes[: is the risk high enough that it actually warrants forcing deals apart.”298 In other words, a large universe of activities must be reviewed, with fine policy distinctions being made after the fact, behind the scenes, on a case-by-case basis. This strategy, typical of the American national security establishment, risks casting a chill over huge swaths of commercial transactions. A more targeted and rigorous approach is needed.

In June 2021, Biden signed an executive order on “Protecting Americans’ Sensitive Data from Foreign Adversaries.”299 This order singles out the threat from China and tasks agencies with making “recommendations to protect against harm from the unrestricted sale of, transfer of, or access to United States persons’ sensitive data, including personally identifiable information, personal health information, and genetic information, and harm from access to large data repositories by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary.” A formal process for grappling with these problems is a welcome improvement on the previous, ad hoc approach. But the ultimate value of this process will depend on whether key terms from Biden’s order can be given more specific, tightly focused definitions. “Sensitive data,” “personally identifiable information,” and “large data repositories” are vague concepts that could easily lead to overreaching governmental controls. These concepts should be refined to include only the highest-priority data, as outlined above.
KEY OFFENSIVE POLICIES

The U.S. government has many opportunities to protect Americans’ personal data from Chinese intelligence, beyond imposing restrictive measures aimed specifically at China. Above all, Congress should establish national data privacy and cybersecurity standards. Many experts have called for federal legislation to replace the weak smattering of sector-specific and state-level rules. With new mega-breaches and data abuses routinely coming to light, it is clear that many U.S. companies lack adequate incentives to protect Americans’ private information. National cybersecurity and data privacy standards would be adversary-agnostic, aiming to stop any malicious actor from wrongfully purchasing or stealing sensitive personal data. By addressing the underlying problem—that Americans’ personal data is very easy to obtain—such standards would do more to thwart Beijing’s intelligence collection than most China-centric measures.

The U.S. government can also take specific precautions to protect its own officials. While all Americans have an interest in preventing Beijing from accessing their personal data, the most acute national security threat is Chinese intelligence targeting those with classified information—a much narrower category. In response to this growing threat, U.S. agencies have significantly increased their China-related counterintelligence activities. Still, the scope of the problem described by U.S. officials calls for even more resources. The government should step up its monitoring and disruption of Chinese intelligence operations, provide more frequent and detailed defensive counterintelligence briefings, and hand down new guidance or restrictions for officials’ use of higher-risk online spaces like LinkedIn, among other possibilities. Targeted counterintelligence programs, while often not sufficient on their own, can help advance U.S. policy objectives without many of the costs and risks that come with broad-based technology restrictions.

**National cybersecurity and data privacy standards, although adversary-agnostic, would do more to thwart Beijing’s intelligence collection than most China-centric measures.**
LIMITING CHINESE NATIONAL SECURITY ESPIONAGE


283 More appropriate protections would include national data security and privacy standards, plus regulations, trainings, and counterintelligence programs specifically focused on the online activities of U.S. military members.


146  U.S.-CHINA TECHNOLOGICAL “DECOUPLING”: A STRATEGY AND POLICY FRAMEWORK