Congressional Testimony

House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party

"Risky Business": Growing Peril for American Companies in China

Piper Lounsbury

Chief Research and Development Officer

Strategy Risks, Corp.

Washington, D.C.

July 13, 2023

Testimony of Piper Lounsbury Before the United States Congress House Select Committee on

Strategic Competition Between the United States and the Chinese Communist Party

Hearing on
"Risky Business": Growing Peril for American Companies in China
July 13, 2023

WRITTEN TESTIMONY

INTRODUCTION

Chairman Gallagher, Ranking Member Krishnamoorthi, and distinguished members of the Select Committee:

I thank you for inviting me to testify today on the day-to-day risks and challenges facing US companies operating in China. I've worked on US-China business issues for nearly 30 years, including 10 years in Beijing. Like me, many US executives with decades of experience trying to work in China have begun to realize that the Communist Party of China (CPC)'s evolving development goals are structured to advance Beijing's stated objective of eventually replacing American firms and businesses while using and subjugating them in the near term.[1] To achieve this goal, the CPC has created a set of national development strategies which rely on theft, coercion and merger-enabled access to US technologies, intellectual property, and data. Yet US shareholders and investors remain unaware - or choose not to look - at the extent to which such practices exist. Since China is now the second-largest country in the world by nominal GDP and the largest country in the world by GDP in purchasing power parity (PPP),[2] American CEOs are increasingly concerned that risk is higher now than ever before.

I'll share a few examples of the types of risk I encountered related to IP acquisition and non-tariff barriers:

1. A PRC mayor of a high-profile mega city demanded a Fortune 100 American CEO release its *latest* high-tech IP to its Chinese partner, or the American firm would lose PRC market access for its other businesses– a direct threat.

2. Another US company's local JV partner stole IP from the US partner to establish a local, state-funded competitor factory right across the street - taking not only the IP but also the US firm's marketing and distribution networks and made it nearly impossible for the US company to exit the joint venture.

3. A US manufacturing factory in a PRC megacity paying tens of millions of dollars in taxes per year to the local government was barred from bidding on a public procurement project worth over $200 million just

[1] Communist Party of China (CPC) is the self-designated correct English name of the PRC's ruling party. Pointe Bello LLC: "On Pointe: To Effectively Meet Challenges the PRC Ruling Party Poses, Learn and Use its *True Name*," posted November 2020 on the official website of Pointe Bello LLC, observed July 11th, 2023, at URL: https://www.pointebello.com/insights/prc-ruling-partys-true-name, archived at: https://web.archive.org/web/20230711183355/https://www.pointebello.com/insights/prc-ruling-partys-true-name.
[2] "GDP: All countries and economies," The World Bank, undated, observed July 11th, 2023, at: https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?view=map, archived at: https://web.archive.org/web/20230711183045/https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?view=map.

because the state-owned competitor did not want US brand competition. The same case was allegedly tied to an illicit settlement payoff linked to a wrongful death blamed on the same US company. If the US company had not paid the settlement, the bid award would have been granted to the local firm. Some would call this extortion. But this is what day to day life is like for US executives in China.

RISKS ARE INTENSIFYING

Now, doing business with China is structurally so different across our two political and economic systems with an overwhelming power asymmetry that it is a fantasy to imagine we can come together in a shared and equitable partnership unless we come together under the PRC's terms, in other words unless we get absorbed by the Communist Party of China and its converted subjects.

To highlight this point, the CEO of Raytheon Technologies expressed in a media interview that the US needs to find a way to get along with China considering the $500 billion dollars of trade flow from China to the US, and that de-risking is impractical because China is "too big, too important, and too necessary for the US economy," he remarked.[3] Most Fortune 100 companies have invested trillions of dollars in the PRC since the 1980s, so indeed, protecting US investments requires the US getting along with China. However, the "terms of service" for doing business with the PRC have changed so considerably in just the last decade creating a power asymmetry and new data monopoly favoring the CPC that any US business investments with the PRC are in peril for the following reasons:

Beijing creating global data monopoly, simultaneously blocking foreign access to PRC data . . .

PRC authorities can now charge any domestic or foreign business or person with "espionage" simply for providing any services using PRC-origin information to third country-based customers.[4] Beijing's recent crackdowns on US consulting businesses as well as Beijing's enhanced data secrecy laws limiting the flow of PRC information highlight the adverse asymmetry for US and other foreign companies trying to conduct business in the PRC.[5][6][7][8] This means that companies requiring due diligence in advance of a business transaction – a

[3] "Raytheon CEO: It's important to understand that we have to find a way to get along with China", posted June 20th, 2023, Squawk Box, *CNBC News,* observed June 30th, 2023, at: https://www.cnbc.com/video/2023/06/20/raytheon-ceo-its-important-to-understand-that-we-have-to-find-a-way-to-get-along-with-china.html, archived at: https://web.archive.org/web/20230701005118/https://www.cnbc.com/video/2023/06/20/raytheon-ceo-its-important-to-understand-that-we-have-to-find-a-way-to-get-along-with-china.html.

[4] On April 26, 2023, the 2nd Session of the 14th Standing Committee of NPC made revisions to the PRC's Counter Espionage Law (CEL [新修正的中华人民共和国反间谍法]) that was originally adopted and enacted on November 1, 2014. *Xinhuanet* [新华网]: ""(Authorized Promulgation) Counter-espionage Law of the People's Republic of China [（受权发布）中华人民共和国反间谍法], published April 26th, 2023, *Xinhuanet* [新华网], observed May 6th, 2023, at: http://www.news.cn/politics/2023-04/26/c_1129569081.htm.

[5] Associated Press: "Foreign Companies in China Face Growing Scrutiny, Pressure", posted April 28th, 2023, observed May 5th, 2023, at: https://apnews.com/article/china-foreign-business-corruption-investigation-technology-113adfa55788aabb11896d8b059b32bc**;** Archived at: https://archive.ph/uKi37.

[6] Martina, Michael and Tian Yew Lun, "China detains staff, raids office of US due diligence firm Mintz Group", posted March 24th, 2023, *Reuters,* observed July 11th, 2023, at: https://www.reuters.com/world/us-due-diligence-firm-mintz-groups-beijing-office-raided-five-staff-detained-2023-03-24/, archived at: https://web.archive.org/web/20230711183518/https://www.reuters.com/world/us-due-diligence-firm-mintz-groups-beijing-office-raided-five-staff-detained-2023-03-24/.

[7] Palmer, Elizabeth and Zhang Shuai, "As China raids U.S. businesses and arrests workers, the corporate landscape is getting 'very risky'", posted June 6th, 2023, *CBS News,* observed July 11th, 2023, at: https://www.cbsnews.com/news/china-raids-arrests-us-business-capvision-bain-mintz-group-security-crackdown/, archived at: https://web.archive.org/web/20230711184152/https://www.cbsnews.com/news/china-raids-arrests-us-business-capvision-bain-mintz-group-security-crackdown/.

[8] Pierson, David and Daisuke Wakabayashi, "China's Crackdown Widens as Police Raid Another Firm with Foreign Ties", posted May 8th, 2023, *The New York Times,* observed July 11th, 2023, at: https://www.nytimes.com/2023/05/08/business/capvision-china-espionage-law.html, archived at: https://web.archive.org/web/20230711184538/https://www.nytimes.com/2023/05/08/business/capvision-china-espionage-law.html.

normal business function in any other country - can no longer conduct such investigations. Additionally, due to the China's Personal Information Protection Law, US companies have been unable to send PRC customer use data to their US headquarters, affecting safety concerns, quality reports, system upgrades, and market use data.[9]

- PRC data security laws and regulations—together with plans issued by Ministries and Commissions—appear intended to advance the CPC's Leninist goal to gain global monopoly over the availability and content of business information. For example, the June 2021 Data Security Law (DSL [中华人民共和国数据安全法]) appears to create a huge negative impact on freedom of access to information about PRC businesses, with business data platforms based in the PRC increasingly blocking persons lacking PRC government-issued identification from accessing their services.[10]

- Article 33 of the DSL stipulates that when providing services, data transaction intermediaries shall require data providers to specify the sources of the data, verify the identities of both parties to the transactions, and retain the verification and transaction records.

- Article 36 of the DSL stipulates that organizations and individuals in the PRC must obtain the approval of the "competent authority" when dealing with cross-border data submission requests made by foreign judicial or law enforcement authorities. The "competent authority" [主管机关] in this Article can refer to MSS, MPS, Ministry of Commerce, State Council and other government agencies from central to provincial level governments depending on the circumstances and severity of the case under review.

- Under Article 36 of the DSL, foreign businesses likely will face difficulties in potential court cases or forced labor-related due diligence work with their PRC-based suppliers and or business partners. The 'competent authority' can easily classify the data needed for foreign judicial or law enforcement situations under "sensitive", "national security" or "data sovereignty"-related terms. This is also likely to create extra hurdles for foreign businesses [engaged/to enforce claims] in business disputes with PRC entities.

- In addition to enacting data secrecy laws, Beijing has advanced complementary policy initiatives aimed at proactively limiting outsider access to business data. For example, the State Administration for Market Regulation (SAMR) announced a "National Pilot Work Plan for the Protection of Commercial Secrets" in March 2022, and in July SAMR law enforcement officers held a "study and research meeting" with Douyin (TikTok's parent company) at its headquarters in Haidian District of Beijing, to discuss a "Commercial Secrecy Pilot project." [11] [12]

---

[9] The NPC of the PRC Website [全国人大网]: "Personal Information Protection Law of the People's Republic of China [中华人民共和国个人信息保护法]," posted August 20th, 2021on the official website of the NPC, observed July 11th, 2023, at URL: http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml and archived at: https://web.archive.org/web/20230711081359/http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

[10] The NPC of the PRC Website [全国人大网]: "PRC Data Security Law" [中华人民共和国数据安全法], posted June 10th, 2021 at URL http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml, archived at: https://web.archive.org/web/20230411065530/http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml.

[11] State Administration for Market Regulation [国家市场监督管理总局]: "Notice of the State Administration for Market Regulation on Printing and Distributing the National Pilot Work Plan for the Protection of Commercial Secrets [市场监管总局关于印发全国商业秘密保护创新试点工作方案的通知]" published March 2nd, 2022, by the State Administration for Market Regulation [国家市场监督管理总局] , rehosted March 2nd, 2022, by the PRC government official website [www.gov.cn], observed July. 11th 2023 at URL: http://www.gov.cn/zhengce/zhengceku/2022-03/23/content_5680784.htm, archived at: https://web.archive.org/web/20230711214656/https://www.gov.cn/.

[12] Beijing City Haidian District Peoples Government [北京市海淀区人民政府]: "Wang Jun, head of the Haidian District Market Supervision Comprehensive Law Enforcement Brigade, led a team to Beijing Douyin Information Service Co., Ltd. to conduct research [海淀区市场监管综合执法大队大队长王军带队到北京抖音信息服务有限公司开展调研]" posted August 15th, 2022, official website of Beijing City Haidian District

. . . and invasively collecting the business, personal, and logistics data of other nations.

But while the PRC has locked down access to its data, the CPC is attempting to extensively collect, store and exploit big data from the US, especially the Personally Identifiable Information (PII) of Americans and USA Allies (including biometrics used in "secure ID"). The lucrative business model of collecting and selling personal data is a national security concern for the US. As major identity technology service providers are often multinational corporations operating across continents, there is a pressing need for oversight in how/where the data is being stored, used, and accessed. I have seen that US government identity technology service providers who have access to US citizen's biometric information and works closely with the US Federal Government, have close business ties with the CPC. Some of these firms have a track record of providing services/equipment, such as their biometric security products, to the agencies in the PRC's Ministry of Public Security (MPS). The MPS's roles include intelligence collection, and the MPS has been involved with systematic human rights abuses, such as the ongoing repression of Uyghurs in Xinjiang, as well as transnational harassments of PRC dissidents in the US.

For example, IDEMIA—the US Government's (USG) key partner in identity technology and biometric data—currently has a substantial physical and digital presence in the People's Republic of China (PRC), with a track record of partnering with CPC State-owned enterprises (SOEs) for over 20 years.[13] Today, the biometric and personal identifiable information (PII) data of US citizens are increasingly accessed and used by US federal & local authorities. Usages of such data include the identification, security, and authentication of purposes of travel, social services, social security, as well as law enforcement.[14] US government contracts for these projects are being granted to private corporations with deep industry ties to the Communist Party of China (CPC), such as IDEMIA. Augmented by Beijing's recent crackdown on foreign businesses as well as changes to its data privacy laws, IDEMIA's close relationship with the CPC constitutes a major risk for the data security and PII privacy of US citizens.

- IDEMIA Identity & Security USA LLC, formerly Morpho (MorphoTrust USA), also known as Sagem and Safran Identity & Security, is the US arm of the French multinational conglomerate, IDEMIA Group

observed July 11th, 2023, at: https://zyk.bjhd.gov.cn/jbdt/auto4504_56266/auto4504_53332/auto4504/auto4504/202208/t20220815_4548283.shtml, archived at:
https://web.archive.org/web/20230711214812/https://zyk.bjhd.gov.cn/jbdt/auto4504_56266/auto4504_53332/auto4504/auto4504/202208/t20220815_4548283.shtml.

[13] Morpho Detection, "Morpho supplies Chinese airports with advanced explosives detection solutions", posted June 17th, 2015, *Global Newswire*, observed June 27th, 2023, at: https://www.globenewswire.com/en/news-release/2015/06/17/1073000/0/en/Morpho-Supplies-Chinese-Airports-With-Advanced-Explosives-Detection-Solutions.html, archived at: https://web.archive.org/web/20230627200818/https://www.globenewswire.com/en/news-release/2015/06/17/1073000/0/en/Morpho-Supplies-Chinese-Airports-With-Advanced-Explosives-Detection-Solutions.html.; "Mobile authentication in China more secure and convenient with biometric solutions from Uni-ID and Safran Identity & Security", undated, Morpho Dys Official Website, observed June 27th, 2023, at: https://morphodys.com/en/reference.php, archived at:
https://web.archive.org/web/20230627200540/https://morphodys.com/en/reference.php.

[14] Lynch, Jennifer, "TSA plans to use face recognition to track Americans through airports", published Nov. 9th, 2017, *Electronic Frontier Foundation*, observed June 26th, 2023, at: https://www.eff.org/deeplinks/2017/11/tsa-plans-use-face-recognition-track-americans-through-airports, archived at: https://web.archive.org/web/20230626184409/https://www.eff.org/deeplinks/2017/11/tsa-plans-use-face-recognition-track-americans-through-airports. ; "IDEMIA continues long-standing partnership with Florida Department of Law Enforcement to deliver world-leading MBIS cloud technology", posted March 9th, 2023, *PR Newswire,* observed June 27th, 2023, at: https://www.prnewswire.com/news-releases/idemia-continues-long-standing-partnership-with-florida-department-of-law-enforcement-to-deliver-world-leading-mbis-cloud-technology-301768150.html, archived at: https://web.archive.org/web/20230627192305/https://www.prnewswire.com/news-releases/idemia-continues-long-standing-partnership-with-florida-department-of-law-enforcement-to-deliver-world-leading-mbis-cloud-technology-301768150.html.

(IDEMIA).[15] IDEMIA has had several subsidiaries within the People's Republic of China (PRC) manufacturing and providing support/services for its biometric surveillance products worldwide. Furthermore, due to the wide range of biometric security and technology products that IDEMIA's corporate group develops, its ties with the CPC's national security apparatus and other SOEs have been shown to be highly intertwined. This is particularly salient in the aviation, consumer mobile devices, and payment transaction industries.

- As of June of 2023, IDEMIA has two operational subsidiaries located within the PRC on listed its website.[16] These include a factory in Shenzhen and a support & service center in Hong Kong SAR. Previously, Morpho Security Systems (莫弗安全系统), the official name of IDEMIA's subsidiary in the PRC between 2004 – 2020, owned multiple operations and subsidiary entities across Mainland China, including in Beijing, Shanghai, Shenzhen and Wuhan.[17]

- According to a September 2020 report by Amnesty International, IDEMIA supplied facial recognition equipment to the Shanghai Public Security Bureau in 2015.[18] Despite the report mentioning that, since then IDEMIA has identified the "human rights risks associated with exports of surveillance technology to China". However, IDEMIA's most recent CSR Report from December 2021 shows no such reference or indication of such risks.[19] On the contrary, in the report's appendix, the PRC is listed officially as a "significant manufacturing site" for IDEMIA operations globally.[20]

- IDEMIA's corporate predecessor, Safran Identity & Security, was a branch of Safran S.A, the French multinational conglomerate specializing in aerospace and defense. Safran was—and still is to this day—deeply embedded in the PRC's aviation market, alongside its consumer mobile device and payment transaction industries.[21] Furthermore, according to the LinkedIn profiles of Safran employees, local hires in

---

[15] "Safran groups companies under a single brand", posted May 19th, 2016, on IDEMIA official website, observed June 26th, 2023, at: https://www.idemia.com/press-release/safran-groups-companies-under-single-brand-2016-05-19, archived at: https://web.archive.org/web/20230627144956/https://www.idemia.com/press-release/safran-groups-companies-under-single-brand-2016-05-19.

[16] IDEMIA's locations worldwide, undated, IDEMIA official website, observed June 27th, 2023, at: https://www.idemia.com/locations#info78, archived at: https://web.archive.org/web/20230627150905/https://www.idemia.com/locations.

[17] IDEMIA (Shenzhen) Co. Ltd., 爱德觅尔(深圳)科技有限公司, undated, Aliyun business database, observed June 27th, 2023, at: https://market.aliyun.com/qidian/company/1180716047950533749, archived at: https://web.archive.org/web/20230627150321/https://market.aliyun.com/qidian/company/1180716047950533749; Morpho Security Systems (Shanghai) Co. Ltd., 莫弗安全系统(上海)有限公司武汉分公司, undated, Aliyun business database, observed June 27th, 2023, at: https://market.aliyun.com/qidian/company/1180716083876194782, archived at: https://web.archive.org/web/20230627165049/https://market.aliyun.com/qidian/company/1180716083876194782.

[18] "Out of Control: Failing EU Laws for Digital Surveillance Export", published Sep. 21st, 2020, by *Amnesty International,* pg. 25, observed June 27th, 2023, at: https://www.amnesty.org/en/latest/press-release/2020/09/eu-surveillance-sales-china-human-rights-abusers, archived at: https://web.archive.org/web/20230627203646/https://www.amnesty.org/en/documents/EUR01/2556/2020/en/.

[19] "Corporate Social Responsibility Report, January – December 2021", undated, IDEMIA, observed June 27th, 2023, at: https://www.idemia.com/wp-content/uploads/2021/02/idemia-csr-report-202207.pdf, archived at: https://web.archive.org/web/20230627203914/https://www.idemia.com/wp-content/uploads/2021/02/idemia-csr-report-202207.pdf.

[20] "Corporate Social Responsibility Report, January – December 2021, Appendix: Global Reporting Initiative References", undated, IDEMIA, observed June 27th, 2023, at: https://www.idemia.com/wp-content/uploads/2021/09/idemia-global-reporting-initiative-guidelines-202207.pdf, archived at: https://web.archive.org/web/20230627204032/https://www.idemia.com/wp-content/uploads/2021/09/idemia-global-reporting-initiative-guidelines-202207.pdf.

[21] "China", undated, Safran official website, observed June 30th, 2023, at: https://www.safran-group.com/countries/china, archived at: https://web.archive.org/web/20230630144746/https://www.safran-group.com/countries/china; "Uni-ID and Safran Identity & Security to make mobile authentication in China more secure and convenient with biometrics", March 1st, 2017, Safran official website, observed June 30th, 2023, at: https://www.safran-group.com/pressroom/uni-id-and-safran-identity-security-make-mobile-authentication-china-more-secure-and-convenient-2017-03-01, archived at: https://web.archive.org/web/20230630144912/https://www.safran-group.com/pressroom/uni-id-and-safran-identity-security-make-mobile-authentication-china-more-secure-and-convenient-2017-03-01.

the PRC have been personnel coming from the PRC's Ministry of Public Security and Public Security Bureau.[22] Even after IDEMIA officially separated its corporate structure from Safran in September 2016, IDEMIA continued to partner with leading Chinese tech providers, such as Lenovo in sharing and integrating biometric technology.[23] Lenovo is owned by the Chinese Academy of Sciences (CAS)—which is on the US Department of Commerce's Entity List—and other PRC institutional investors.[24]

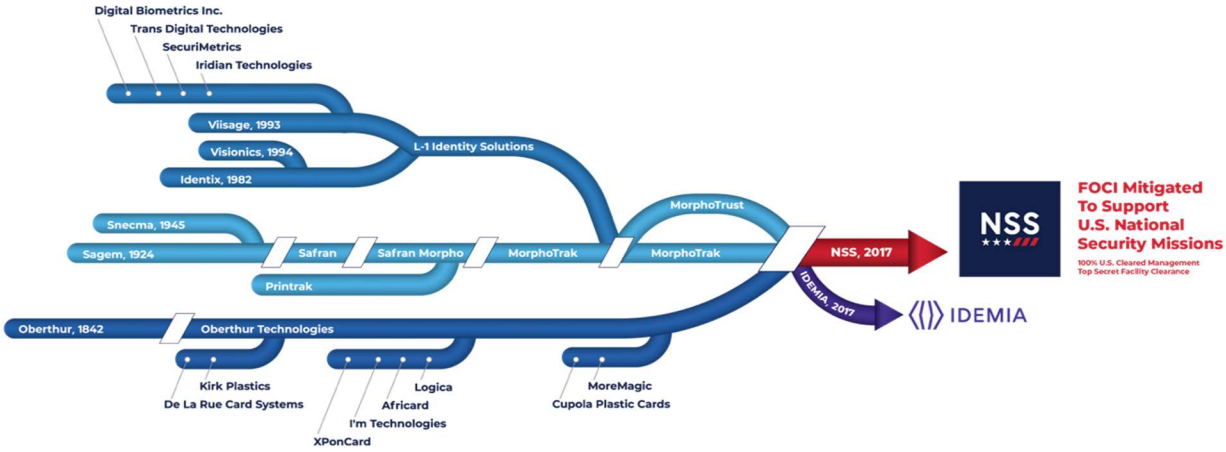
- IDEMIA is the official enrollment provider of TSA PreCheck, as well as a wide range of federal and local government partnerships nationwide.[25] In March of 2023, David Pekoske, Administrator of the TSA expressed during an interview SXSW 2023 TSA's intention that: "eventually we will get to the phase where we require biometrics across the board".[26] Furthermore, the scale of IDEMIA's enrollment operations is ubiquitous across the US, as its physical enrollment centers are in over 560 locations nationwide.[27] IDEMIA's biometric technology is currently in 16 airports across the US. PBS and the Associated Press reports that it is being used at "Reagan National near Washington, D.C., airports in Atlanta, Baltimore, Boston, Dallas, Denver, Detroit, Las Vegas, Los Angeles, Miami, Orlando, Phoenix, Salt Lake City, San Jose, and Gulfport-Biloxi and Jackson in Mississippi."[28]

- Additionally, IdentoGO by IDEMIA, is the prime secure identity-related services provider across most US states and territories. Providing "digital fingerprinting services" for government agencies in social services, employment, financial and health services. According to their website, their "primary service [is] the secure

[22] "Xin Hu LinkedIn Profile", undated, LinkedIn, observed June 29th, 2023, at: https://www.linkedin.com/in/xin-hu-0550737b/?originalSubdomain=cn, archived at:
https://web.archive.org/web/20230629174814/https://www.linkedin.com/authwall?trk=gf&trkInfo=AQFkybA4jUs9TgAAAYkIRRsw22nSJ0XpRhjySBreaeQXYb81cmfkFfzvwvMRjoSokWoDnMhYyOibnOX4RsThwnThz-MSm5afT3IbavExwIjA5S3NbkBU6sHg4fh-T-N9hoLDcWQ=&original_referer=&sessionRedirect=https%3A%2F%2Fwww.linkedin.com%2Fin%2Fxin-hu-0550737b%2F%3ForiginalSubdomain%3Dcn.
[23] "Uni-ID and Safran Identity & Security to make mobile authentication in China more secure and convenient with biometrics", posted March 1st, 2017, on IDEMIA official website, observed June 29th, 2023, at: https://www.idemia.com/press-release/uni-id-and-safran-identity-security-make-mobile-authentication-china-more-secure-and-convenient-biometrics-2017-03-01?export=pdf&post_id=3309&force, archived at:
https://web.archive.org/web/20230629171224/https://www.idemia.com/press-release/uni-id-and-safran-identity-security-make-mobile-authentication-china-more-secure-and-convenient-biometrics-2017-03-01?export=pdf&post_id=3309&force.
[24] "Entity List", updated on May 19th, 2023, Bureau of Industry and Security, US Department of Commerce, pg. 100, observed June 29th, 2023, at: https://www.bis.doc.gov/index.php/documents/regulations-docs/2326-supplement-no-4-to-part-744-entity-list-4/file, archived at:
https://web.archive.org/web/20230629172642/https://www.bis.doc.gov/index.php/documents/regulations-docs/2326-supplement-no-4-to-part-744-entity-list-4/file.
[25] "IDEMIA in the USA", undated, IDEMIA official website, observed June 28th, 2023, at: https://www.idemia.com/usa, archived at:
https://web.archive.org/web/20230628141125/https://www.idemia.com/usa.; "TSA enrollment by IDEMIA", undated, *IdentoGo by IDEMIA,* observed June 27th, 2023, at: https://www.identogo.com/services/tsa-programs, archived at:
https://web.archive.org/web/20230627194714/https://www.identogo.com/services/tsa-programs.
[26] "Accelerating Aviation Security: Innovative New Technology Keeping the Skies Safe", posted March 14th, 2023, *SXSW* Official Website, observed June 27th, 2023, at: https://schedule.sxsw.com/2023/events/PP1143589, archived at:
https://web.archive.org/web/20230627204748/https://schedule.sxsw.com/2023/events/PP1143589.
[27] IDEMIA Identity & Security USA LLC, "IDEMIA Identity and Security North America enrolls in TSA PreCheck at over 560 enrollment centers nationwide", posted June 26th, 2023, on *PR Newswire*, observed June 27th, 2023, at: https://www.prnewswire.com/news-releases/idemia-identity-and-security-north-america-enrolls-in-tsa-precheck-at-over-560-enrollment-centers-nationwide-301863508.html, archived at:
https://web.archive.org/web/20230627210622/https://www.prnewswire.com/news-releases/idemia-identity-and-security-north-america-enrolls-in-tsa-precheck-at-over-560-enrollment-centers-nationwide-301863508.html.
[28] Santana, Rebecca, "TSA is testing facial recognition technology at more airports, raising privacy concerns", published May 15th, 2023, *PBS News Hour,* observed June 27th, 2023, at: https://www.pbs.org/newshour/politics/tsa-is-testing-facial-recognition-technology-at-more-airports-raising-privacy-concerns, archived at: https://web.archive.org/web/20230627205909/https://www.pbs.org/newshour/politics/tsa-is-testing-facial-recognition-technology-at-more-airports-raising-privacy-concerns.

capture and transmission of electronic fingerprints".[29] In June of 2022, IDEMIA announced that it has been able to develop biometric ID and smart cards deployable for mass production.[30]

- Another IDEMIA USA subsidiary, IDEMIA National Security Solutions LLC (IDEMIA NSS) currently partners with the US military in our nation's "most critical facilities".[31] IDEMIA NSS claims to be the "foreign ownership, control, or influence (FOCI) mitigated IDEMIA affiliate" and operates under a special security agreement (SSA) with the Department of Defense.[32]



(Image 1: About US, IDEMIA NSS Official Website)[33]

- IDEMIA's misuse of biometric data and PII collection of US citizens, along with its history of collaboration with PRC state entities, points to the highest level of risk exposure from foreign actors, especially the CPC.

- In December 2017, allegations arose that IDEMIA's fingerprint-recognition technology (then developed by Safran) which was sold to the FBI contained Russian code, which was "deliberately concealed" during the sale.[34] The case is currently on appeal, however since then, the DOJ's most recent audit of FBI purchase orders found that the ongoing partnership between IDEMIA and the FBI "contained insufficient

[29] "About Us", undated, IdentoGO official website, observed June 29th, 2023, at: https://www.identogo.com/about, archived at: https://web.archive.org/web/20230629180545/https://www.identogo.com/about.
[30] "Biometric cards, making convenience secure", posted June 30th, 2022, IDEMIA official website, observed June 29th, 2023, at: https://www.idemia.com/insights/biometric-cards-making-convenience-secure, archived at: https://web.archive.org/web/20230629181543/https://www.idemia.com/insights/biometric-cards-making-convenience-secure.
[31] "Insights", undated, IDEMIA NSS official website, observed June 29th, 2023, at: https://www.idemia-nss.com/insights/, archived at: https://web.archive.org/web/20230629190104/https://www.idemia-nss.com/insights/.
[32] "Defense Industrial Security: Special Security Agreements Permit Foreign-owned U.sS. Firms to Perform Classified Defense Contracts", published March 21st, 1990, US Government Accountability Office (GAO), observed June 29th, 2023, at: https://www.gao.gov/products/t-nsiad-90-17, archived at: /web/20230629190901/https://www.gao.gov/products/t-nsiad-90-17.
[33] "About", IDEMIA National Security Solutions, undated, observed June 30th, 2023, at: https://www.idemia-nss.com/about/, archived at: https://web.archive.org/web/20230630145520/https://www.idemia-nss.com/about/.
[34] Hamby, Chris, "FBI software for analyzing fingerprints contains Russian-made code, whistleblowers say", posted Dec. 26th, 2017, *BuzzFeed* News, observed June 29th, 2023, at: https://www.buzzfeednews.com/article/chrishamby/fbi-software-contains-russian-made-code-that-could-open-a, archived at: https://web.archive.org/web/20230629182918/https://www.buzzfeednews.com/article/chrishamby/fbi-software-contains-russian-made-code-that-could-open-a.

documentation" and that the "noncompetitive simplified acquisition procedures" the FBI used was improper.[35]

- IDEMIA's initial CFIUS review, assessing the merger between Paris-based Safran and US-based L-1 Identity Solutions in July 2011 allowed IDEMIA to "operate its software development and maintenance of programs domestically in the US".[36] However, recent developments and findings shows that foreign interference and exposure in IDEMIA's supply chain may provide Beijing with a back channel, compromising the security of biometric and PII data of US citizens.[37]

And in addition to biometric data, Beijing intends to globally ingest, monopolize, and control all international supply chain logistics data in the PRC's "national logistics information platform [国家物流信息平台]" LOGINK, *aka* "national transportation and logistics public information platform." A December 2022 State Council opinion called for PRC entities to "participate deeply in the formulation of international digital rules."[38] The CPC has been developing LOGINK since 2007 with the goal of persuading global logistics corporations to enter more if not all of their data into LOGINK, which Beijing hopes will provide the PRC with hegemonic visibility not only into the data of its own shippers but also into the flow of goods through every other logistics system on earth.[39]

The CPC has designed LOGINK to collect and store global participants' price and tracking information for cross-sector, cross-regional, cross-border, private-to-public, public-to-private data query, verification, or exchange. The PRC offers LOGINK to global participants at "no cost" in return for participants' fusion/provision of their data systems with LOGINK, as well as adoption of LOGINK standards by users, and is cultivating a substantial first mover advantage as a central hub for global logistics information exchange.[40] Indicating that it will likely use LOGINK to collect business and other intelligence on the USA, the CPC

---

[35] "Audit of the Federal Bureaus of Investigation's Biometric Algorithm Purchase Order Awarded to Idemia National Security Solutions, LLC", Feb. 2022, Department of Justice, Office of the Inspector General, observed June 29th, 2023, at: https://oig.justice.gov/sites/default/files/reports/22-045.pdf, archived at: https://web.archive.org/web/20230629183815/https://oig.justice.gov/sites/default/files/reports/22-045.pdf.

[36] "Safran completes $1 billion face-recognition deal" posted July 26th, 2011, *Reuters,* observed June 29th, 2023, at: https://www.reuters.com/article/us-l1-safran/safran-completes-1-billion-face-recognition-deal-idUSTRE76P36720110726, archived at: https://web.archive.org/web/20230629185153/https://www.reuters.com/article/us-l1-safran/safran-completes-1-billion-face-recognition-deal-idUSTRE76P36720110726.

[37] Krishan, Nihal, "French ID security contractor exposed data of millions of US citizens, whistleblower alleges", posted Nov. 10, 2023, *Washington Examiner,* observed June 29th, 2023, at: https://www.washingtonexaminer.com/policy/french-id-security-contractor-exposed-data-of-millions-of-us-citizens-whistleblower-alleges#:~:text=A%20French%20identity%2Dverification%20security,filed%20by%20a%20company%20whistleblower., archived at: https://web.archive.org/web/20230629185401/https://www.washingtonexaminer.com/policy/french-id-security-contractor-exposed-data-of-millions-of-us-citizens-whistleblower-alleges.

[38] People's Daily Website [人民网－人民日报]: "Opinions of the Central Committee of the Communist Party of China and the State Council on Building a Basic Data System and Making Better Use of Data Elements [中共中央国务院关于构建数据基础制度更好发挥数据要素作用的意见]" posted Dec. 2nd, 2022, on the People's Daily Website [人民网－人民日报], observed July 11th, 2023, at: http://politics.people.com.cn/n1/2022/1220/c1001-32589920.html, archived at: https://web.archive.org/web/20230711215503/http://politics.people.com.cn/n1/2022/1220/c1001-32589920.html.

[39] Wheeler, Andre, "China's LOGINK digital platform: a weapon to bring about a new economic hegemon through data control, ownership, and manipulation?" posted Oct. 5th, 2022, *Asia Power Watch: An observatory of Asia-Pacific economic power*, observed May 8th, 2023, at: https://asiapowerwatch.com/chinas-logink-digital-platform-a-weapon-to-bring-about-a-new-economic-hegemon-through-data-control-ownership-and-manipulation/, archived at: https://web.archive.org/web/20230711215605/https://asiapowerwatch.com/chinas-logink-digital-platform-a-weapon-to-bring-about-a-new-economic-hegemon-through-data-control-ownership-and-manipulation/.

[40] Gu Jingyan, Director of the Transport and Logistics Research Center, Research Institute of Highway, Ministry of Transport: "National Transport and Logistics Information Platform in China LOGINK," dated 10 December 2015, observed July 11th, 2023, at: https://www.unescap.org/sites/default/files/01%20-%20LOGINK.pdf, archived at: https://web.archive.org/web/20230711215654/https://www.unescap.org/sites/default/files/%2001%20-%20LOGINK.pdf. (According to Gu, LOGINK does assess a charge for a greater "value-added" service level of the platform which provides access to mining of LOGINK data.)

administers LOGINK through nine ministries—including the Ministry of Industry and Information Technology (MIIT[工业和信息技术部]) while the CPC has moved increasingly in recent years to hide this and other data from access by those outside the PRC that it does not control or favor, through its raft of successive laws dictating data secrecy.

- LOGINK supports multiple key PRC national development strategies that seek to bolster Beijing's global power and influence, including by controlling global information and communications technology (ICT) in line with the Digital Silk Road Initiative, a key pillar of Beijing's One Belt One Road (OBOR) *aka* Belt and Road Initiative (BRI), which in turn is the top priority of the CPC's Regional Coordination Development Strategy [区域协调发展战略]. Beijing's Military Civil Fusion Development Strategy (MCF [军民融合发展战略]) aligns with LOGINK and broader PRC logistics and transportation objectives under OBOR points to potential security risks, including economic espionage, surveillance (e.g., U.S. and allied military movements/deployments), and disruption threats (e.g., selectively shutting down critical infrastructure systems during a conflict).

- LOGINK is nominally administered by the China Transport Telecommunication & Information Center (CTTIC [中国交通通信信息中心])—nominally housed in PRC Ministry of Transportation (MOT)—according to the LOGINK Management Center's "Platform introduction,"[41] By the time the CPC reassigned operational management of LOGINK to CTTIC in 2019, however, CTTIC already operated under authorities granted by the Ministry of Industry and Information Technology (MIIT[工业和信息技术部]), according to information found in reports cached or archived by international portals and/or rehosted on other PRC entities' websites.

- LOGINK in 2019 became a member of International Port Community System Association (IPCSA), an international sectoral organization that it had already been cooperating with for at least two years, paving the way for LOGINK and the PRC's East Asia component of LOGINK (the Northeast Asia Logistics Information-Sharing Network (NEAL-NET [东北亚物流信息服务网络])) to expand to Europe. The membership agreement was signed at the 2019 Port Technology International Smart Digital Ports Conference in Rotterdam; "In cooperation with IPCSA, LOGINK has expanded its logistics information sharing service to Europe; it has connected the Port of Barcelona, Port of Abu Dhabi and is working in cooperation with the ports of Antwerp, Rotterdam, Bremen, and Hamburg. In addition, a logistics information sharing network along the Belt and Road Initiative region is under construction," according to a 2019 Port Technology International article.[42]

- On 11 April 2022, LOGINK joined IPCSA's Network of Trusted Networks (NoTN); IPCSA's secretary general stated that NoTN "provides a secure platform for global data exchange using trusted Port Community Systems or Single Windows. "[43] IPCSA's secretary general continues "Everyone is in control of

[41] LOGINK [national transportation and logistics public information platform] management center [国家交通运输物流公共信息平台管理中心]]: "Platform Overview [平台概况]," undated (copyright 2007-2016), observed July 11th, 2023, at: http://www.logink.cn/col/col38/ index.html, archived at: https://web.archive.org/web/20230711220157/https://www.logink.cn/col/col38/%20index.html.
[42] "China's LOGINK inaugurated into IPCSA", posted Dec. 10th, 2019, Port Technology International, observed July 11th, 2023, at https://www.porttechnology.org/news/chinas-logink-inaugurated-into-ipcsa/, archived at: https://web.archive.org/web/20230711220344/https://www.porttechnology.org/news/chinas-logink-inaugurated-into-ipcsa/.
[43] "LOGINK signs up to IPCSA's Network of Trusted Networks, "IPCSA webpage, April 11th, 2022, at LOGINK signs up to IPCSA's Network of Trusted Networks – IPCSA International, observed July 11th, 2023, at: https://ipcsa.international/news/2022/04/11/logink-signs-up-to-ipcsas-network-

their own data and decides what data they can and will share" but fails to point out that once LOGINK has the data a business or agency choose to connect with LOGINK, that data stream is under PRC control.[44]

- The "Fact Sheet" posted 15 March 2022 by the White House administration about its "Freight Logistics Optimization Works (FLOW)" data sharing partnership "New Initiative" is an opening for LOGINK to entice USA corporations to indirectly or unwittingly join the LOGINK system.[45] The "Fact Sheet" names the Port of Los Angeles among the "Industry partners"—also referred to as FLOW participants—in the "new initiative." The Port of Los Angeles became the first US member of the IPCSA, according to a 17 September 2018 article posted on the Port of Los Angeles website, indicating that the FLOW initiative is at least potentially connected to IPCSA member LOGINK through FLOW participant Port of Los Angeles' membership in IPCSA.[46]

Finally—but by no means least— the CPC's Military Civil Fusion Development Strategy (MCF [军民融合发展战略]) harnesses the data-sharing requirement to harvest USA and other nation's dual-use technologies for use by the PLA, which is how US technology and hardware have found their way into the People's Liberation Army (PLA [人民解放军]) and other state & national security Party organs. For both LOGINK and for MCF, influence over technical standard setting is one of the major vectors that the CPC is using to shift global, multilateral data infrastructure in its own favor at the expense of the USA public, business, and allies. The United States and its allies are just beginning to confront the scope and depth of the threats that these CPC efforts pose. Both can do more to increase recognition and understanding of the comprehensive coordination of CPC efforts to influence and dominate international standards setting entities. The CPC leadership—on the other hand—has spent years organizing and resourcing its plans to manipulate standards for party-and-state benefit, and understands that besides creating operational dominance, setting global standards secures hard currency income by abusing patent values. For example:

- Huawei ties its recent demand for roughly $1 Billion from Verizon to license 238 Huawei patents. Simply wielding myriad patents provides scale, or mass, that empowers legal attacks on competitors, denying them access to consumer and capital markets.
- When Advanced Micro Devices (AMD) faced cash flow challenges, its trove of patents supported a cross-licensing agreement with CPC controlled entities—lucrative in the short term for AMD, strategic for the CPC.

---

of-trusted-networks/, archived at: https://web.archive.org/web/20230711215936/https://ipcsa.international/news/2022/04/11/logink-signs-up-to-ipcsas-network-of-trusted-networks/.

[44] "LOGINK signs up to IPCSA's Network of Trusted Networks, "IPCSA webpage, April 11th, 2022, at LOGINK signs up to IPCSA's Network of Trusted Networks – IPCSA International, observed July 11th, 2023, at: https://ipcsa.international/news/2022/04/11/logink-signs-up-to-ipcsas-network-of-trusted-networks/, archived at: https://web.archive.org/web/20230711215936/https://ipcsa.international/news/2022/04/11/logink-signs-up-to-ipcsas-network-of-trusted-networks/.

[45] White House Briefing Room: "Fact Sheet: Biden-Harris Administration Announces New Initiative to Improve Supply Chain Data Flow," posted March 15th, 2022, the official website of *The White House*, observed July 11th, 2023, at: https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/15/fact-sheet-biden-harris-administration-announces-new-initiative-to-improve-supply-chain-data-flow/ and archived at URL: https://web.archive.org/web/20230708221638/https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/15/fact-sheet-biden-harris-administration-announces-new-initiative-to-improve-supply-chain-data-flow/, archived at: https://archive.ph/AMGK6.

[46] The Port of Los Angeles, "Port of Los Angeles Becomes First U.S. Member of International Port Community Systems Association (IPCSA)", undated The Port of Los Angeles, City of Los Angeles Official Website, observed July 11th, 2023, at: https://www.portoflosangeles.org/references/news_091718_ipcsa, archived at: https://web.archive.org/web/20230711184930/https://www.portoflosangeles.org/references/news_091718_ipcsa.

- Less subtly, the CPC uses standards to export its mechanisms to control populations. In Venezuela, CPC-controlled ZTE mimicked technologies to cross standardize PRC social credit score systems, which not only suppress individuals' freedoms but also helps further coopt undemocratic regimes in support of the CPC's pervasive invasion of privacy practices.
- Beijing aggressively devotes resources to influencing the setting of global standards, suggesting additional resources are needed to strengthen standards support in the United States. Demonstrating geostrategic offense action against public and private interests of the United States and allies, the PRC has built growing leverage within the context of international 5G standards setting.
- In addition to operational dominance and economic benefit to the PRC, China's position poses a significant security risk for the United States and its allies. Huawei drafts patents, identifies security flaws and, also, recommends solutions. Huawei's position allows the CPC to control the entire standards process, which it can use to exploit vulnerabilities for cyber warfare, espionage or for their economic advantage.

RECOMMENDED HIGH PRIORITY CONGRESSIONAL POLICY ACTION OPPORTUNITIES

From business risk in China to personal safety in the US, Congress could play to its own strength by aiming to craft legislation that protect the USA public, including US businesses, their consumers, critical technologies, and supply chains across the board by closing the gaps in the capabilities of US private and public actors to counter moves by CPC-controlled actors. Recommended actions include crafting US legislation and other measures (1) to help Americans and our allies better recognize CPC vectors of risk by promoting the tools, processes and identification of CPC control or influence, (2) to incentivize re-shoring America's supply chain infrastructure outside of the PRC and consider tax or purchase credit incentives to foster supply chain resilience at home, (3) to target generic adverse behaviors and practices of the PRC versus specific enterprises or named programs, and (4) to protect USA data and information from the PRC's global data monopoly behavior.

(1) Help Americans and our allies better recognize CPC vectors of risk.

- Craft US legislation and other measures promoting requirements and incentives to identify CPC control or influence in the private and public institutions of the USA and its allies, as well as the tools, processes, and precision necessary to do so.

- Create requirements for publicly listed companies to publicly disclose revenues generated in the PRC through SEC filings. American companies fudge the numbers. Currently, some include "Mainland China," while others only mention some "Greater China" or "Asia."

- Create requirements for American private equity firms and pension funds to disclose China exposure.

- Create and/or if already created then enforce more rigorous requirements for academic institutions to regularly and publicly disclose funds received from foreign donors as well as tuition paid by foreign students.

- Craft legislation to ensure that the SEC must continue to enforce same due diligence rules and requirements for PRC entities listed on NYSE, NASDAQ, Chicago Commodities Exchange, etc., as for American entities and never again issue "special exception" exempting PRC entities.

(2) Re-shore supply chain infrastructure outside of the PRC and consider tax or purchase credit incentives to foster supply chain resilience.

- Craft legislation and other tax and purchase incentive measures in consultation with US partners and allies to re-shore US supply chain infrastructure outside of the PRC to encourage resilient supply chain development.

- Craft legislation to encourage US businesses to re-evaluate and re-shore their current supply chain infrastructure. For decades, the PRC has been leveraging its gross market capacity and low production costs to increase foreign business' dependency on China. However, Beijing's tendency and intention to monopolize the market through means of coercion and intellectual property theft has been a reoccurring theme across sectors, ranging from rare earth resources to pharmaceuticals to tech to defense.

Recently introduced bills in Congress such as "The Western Hemisphere Nearshoring Act" (H.R. 722) cites the "loss of regional economic opportunity" and the need to "decrease dependency on PRC manufacturing" as the main reasons for nearshoring.[47] Both are true, however, the need to re-shore our supply chains go beyond nearshoring within the Western Hemisphere alone. Rather, this is an opportunity, as well as necessity, to widen the tent and bring in likeminded nations, ensuring cleaner and more resilient supply chains for our most sensitive/critical industries.

The focus should be to diversify "outside of the PRC", rather than simply nearshoring to a particular geographical region. Whilst re-shoring, businesses should also be reminded to consider the long-term resiliency of such an effort. For instance, assessing the risks of re-shoring to locations with close ties to the PRC, such as those with extradition treaties and/or overt political influence from Beijing. As such, the strength, stability, and reliability of local institutions and the rule of law should be top priority in the re-shoring destinations of our supply chains.

Congress should build upon proposed legislation, including the recently introduced "RAM Act of 2023 (Reshoring American Manufacturing, H.R.2571)".[48] Expanding such efforts to include a diverse set of solutions and measures in lockstep with US allies.

The legislation should be crafted and implemented in tandem with our partners and allies. Specifically in the Indo-Pacific and the European Union. Regional institutions or military alliances, such as the QUAD and NATO, should begin promoting and enhancing existing supply chain resilience mechanisms.[49] For

[47] "H.R. 722 – Western Hemisphere Nearshoring Act", Congress.Gov, observed July 11th, 2023, at: https://www.congress.gov/bill/118th-congress/house-bill/722/text, archived at: https://web.archive.org/web/20230711185350/https://www.congress.gov/bill/118th-congress/house-bill/722/text.
[48] "H.R. 2571 – RAM Act of 2023", Congress.Gov, observed July 11th, 2023, at: https://www.congress.gov/bill/118th-congress/house-bill/2571/all-actions?s=1&r=25, archived at: https://web.archive.org/web/20230711185408/https://www.congress.gov/bill/118th-congress/house-bill/2571/all-actions?s=1&r=25.
[49] "NATO 2030: NATO-Private Sector Dialogues with GLOBSEC—Critical Infrastructure and Security of Supply Chains", April 22nd, 2023, GLOBSEC, observed July 11th, 2023, at: https://www.globsec.org/sites/default/files/2021-04/NATO-GLOBSEC-Dialogue-6-Policy-Takeaways.pdf.,

instance, the re-shoring of supply chains specifically for military-use equipment goes beyond domestic US government suppliers and contractors, but extends to our information, technology, and infrastructure sharing agreements with US partners across the globe.

Congress should further consider how legislation could work in conjunction with existing tax policies by major global economic institutions such as the OECD. The recently implemented "Pillar Two" model of 15% global minimum tax by the OECD provides such an example.[50] Incentives such as tax credits, tax breaks , and or purchase credits would encourage businesses to re diversify outside of the PRC's increasingly monopolistic and unreliable marketplace.

(3) Target generic adverse behaviors and practices of the PRC, versus specific enterprises or named programs.

Rather than crafting laws and regulation to sanction Huawei, TikTok, China Communications Construction Company, or Xiaomi, instead craft laws and to sanction any entity that—respectively, and for example—transfers dual use technology to entities that will divert it to military uses, sanction any entity for selling technology with backdoors exploitable for intelligence collection, and sanction any and all entity's collection of personal identifying information (PII).

Laws such as the CHIPS and Science Act and the HFCAA (Holding Foreign Companies Accountable Act) are steps in the right direction, but the CPC's pattern of adapting and detecting loopholes in our constitutional regulatory frameworks shows that their manipulative practices will persist. Beijing's ability to utilize technology and data to enhance their coercive toolkit should prompt us to take decisive and broad measure across the board in countering such actions - beginning with protecting our businesses and our most critical technologies and supply chains.

(4) Protect USA data and information from the PRC's global data monopoly behavior.

Crafting legislation such as the recently introduced the bill H.R.2993 (Preventing PLA Acquisition of US Technology Act of 2023) should be a high priority target to protect the data and information of private and public USA entities.[51] As Ambassador Lighthizer mentioned in his testimony to this committee, Congress should indeed take steps to "prevent current and future technological integration with and dependence on China".[52] This is due not only to fundamentally mercantile trade practices by the PRC, but the fact that

---

archived at: https://web.archive.org/web/20230711185432/https://www.globsec.org/sites/default/files/2021-04/NATO-GLOBSEC-Dialogue-6-Policy-Takeaways.pdf.

[50] Mehboob, Danish and Isabel Gottlieb, "Global Deal's 15% Minimum Tax Seeing Pickup Around the World (Correct)", Feb. 23rd, 2023, Bloomberg Tax, observed July 10th, 2023, at: https://news.bloombergtax.com/daily-tax-report-international/global-deals-15-minimum-tax-seeing-pickup-around-the-world; "OECD releases Pillar Two model rules for domestic implementation of 15% global minimum tax" Dec. 20th, 2021, OECD, observed July 10th, 2023, at: https://www.oecd.org/newsroom/oecd-releases-pillar-two-model-rules-for-domestic-implementation-of-15-percent-global-minimum-tax.htm., archived at: https://web.archive.org/web/20230711185513/https://www.oecd.org/newsroom/oecd-releases-pillar-two-model-rules-for-domestic-implementation-of-15-percent-global-minimum-tax.htm.

[51] "H.R.2993 - Preventing PLA Acquisition of United States Technology Act of 2023", undated, Congress.gov, observed July 7th, 2023, at: https://www.congress.gov/bill/118th-congress/house-bill/2993/text?s=1&r=6, archived at: https://web.archive.org/web/20230707151443/https://www.congress.gov/bill/118th-congress/house-bill/2993/text?s=1&r=6.

[52] Lighthizer, Robert, "Testimony of Robert Lighthizer Before the House Select Committee on Strategic Competition between the United States and the Chinese Communist Party", May 17th, 2023, observed July 7th, 2023, at: https://docs.house.gov/meetings/ZS/ZS00/20230517/115974/HHRG-118-ZS00-Wstate-LighthizerR-20230517.pdf, archived at:

Beijing is simultaneous acting as a data monopolist through a combination of demanding, enticing, buying, stealing or pilfering the data of other nations on the one hand, while on the other hand enforcing protectionism for PRC data, through a raft of laws and regulations and policies. PRC businesses are required by law to share and provide any/all information, data, and technology with Beijing if so requested, while being prevented from sharing data openly—most recently issuing the amended Counter-Espionage Law (CEL [中华人民共和国反间谍法]), under which PRC authorities can charge any domestic or foreign business or person with "espionage" for provide any services using PRC-origin information to third country-based customers.[53] The CPC's Military Civil Fusion Development Strategy (MCF [军民融合发展战略]) harnesses the data-sharing requirement to harvest USA and other nation's dual-use technologies for use by the PLA, which is how US technology and hardware have found their way into the People's Liberation Army (PLA [人民解放军]) and other state & national security Party organs.

A second high priority data and information target for legislation and other countermeasures is the PRC's attempt to extensively collect, store and exploit "big data," especially the PII of Americans and USA Allies (including biometrics used in "secure ID"). Legislation establishing third-party review mechanisms and mandating such reviews may be necessary to protect the Constitutional right to privacy for everyday Americans and their businesses, vis-à-vis for US Government identity technology service providers. The increasingly lucrative business model of collecting and selling personal data is a national security concern for the US. As major identity technology service providers are often multinational corporations operating across continents, there is a pressing need for oversight in how/where the data is being stored, used, and accessed. These companies often do have structural or legal procedures in place to segregate their business operations from outside or third-party access. However, we have seen that government identity technology service providers who have access to US citizen's biometric information and works closely with the US Federal Government, have close business ties with the CPC.[54] Some of these firms have a track record of providing services/equipment, such as their biometric security products, to the agencies in the PRC's Ministry of Public Security (MPS), as well as concealing the possibly adverse code or technology from US

https://web.archive.org/web/20230707151556/https://docs.house.gov/meetings/ZS/ZS00/20230517/115974/HHRG-118-ZS00-Wstate-LighthizerR-20230517.pdf.

[53] *Xinhuanet* [新华网]: "(Authorized Promulgation) Counter-espionage Law of the People's Republic of China [（受权发布）中华人民共和国反间谍法]", published April 26th, 2023, *Xinhuanet* [新华网], observed July 11th, 2023, at: http://www.news.cn/politics/2023-04/26/c_1129569081.htm, archived at: https://web.archive.org/web/20230711220939/http://www.news.cn/politics/2023-04/26/c_1129569081.htm.

[54] IDEMIA (Shenzhen) Co. Ltd., 爱德觅尔(深圳)科技有限公司, undated, Aliyun business database, observed June 27th, 2023, at: https://market.aliyun.com/qidian/company/1180716047950533749, archived at: https://web.archive.org/web/20230627150321/https://market.aliyun.com/qidian/company/1180716047950533749; Morpho Security Systems (Shanghai) Co. Ltd., 莫弗安全系统(上海)有限公司武汉分公司, undated, Aliyun business database, observed June 27th, 2023, at: https://market.aliyun.com/qidian/company/1180716083876194782, archived at: https://web.archive.org/web/20230627165049/https://market.aliyun.com/qidian/company/1180716083876194782.

agencies also buying the services, in sometimes murky acquisition procedures.[55] [56] [57] The MPS's roles include intelligence collection, and the MPS has been involved with systematic human rights abuses, such as the ongoing repression of Uyghurs in Xinjiang, as well as transnational harassments of PRC dissidents in the US.[58]

A third high priority data and information target for legislative protection and other countermeasures is the PRC's campaign to control global logistics data, including that of US supply chains. Legislation is necessary to head off the looming threat of the PRC's developing program which the CPC intends to globally ingest, monopolize and control all international supply chain logistics data, which it deems the "national transportation and logistics public information platform [国家交通运输物流公共信息平台]" or "national logistics information platform [国家物流信息平台]" LOGINK.

Boost the protection of USA entities in the multilateral realm of industrial and technical standards by boosting availability of accurate information, researching, and cataloguing, and analyzing PRC actions (see first recommendation). [59] [60] Specific opportunities for Congress to incentivize US business to research, catalog, and analyze PRC actions include:

- Consider providing a USA federal subsidy to corporations and other institutions which contribute their expert professionals to multilateral standards organizations. Devote additional resources to investigate relationships between the PRC's National Standardization Development Strategy [国家标准化发展战略]and erosion of U.S. market share and economic strength, and potential increased risk of forfeiture of control over DOD equipment and other strategically important infrastructure.

---

[55] "Out of Control: Failing EU Laws for Digital Surveillance Export", published Sep. 21st, 2020, by *Amnesty International,* pg. 25, observed June 27th, 2023, at: https://www.amnesty.org/en/latest/press-release/2020/09/eu-surveillance-sales-china-human-rights-abusers, archived at: https://web.archive.org/web/20230627203646/https://www.amnesty.org/en/documents/EUR01/2556/2020/en/; [55] "Corporate Social Responsibility Report, January – December 2021", undated, IDEMIA, observed June 27th, 2023, at: https://www.idemia.com/wp-content/uploads/2021/02/idemia-csr-report-202207.pdf, archived at: https://web.archive.org/web/20230627203914/https://www.idemia.com/wp-content/uploads/2021/02/idemia-csr-report-202207.pdf.

[56] Hamby, Chris, "FBI software for analyzing fingerprints contains Russian-made code, whistleblowers say", posted Dec. 26th, 2017, *BuzzFeed* News, observed June 29th, 2023, at: https://www.buzzfeednews.com/article/chrishamby/fbi-software-contains-russian-made-code-that-could-open-a, archived at: https://web.archive.org/web/20230629182918/https://www.buzzfeednews.com/article/chrishamby/fbi-software-contains-russian-made-code-that-could-open-a.

[57] "Audit of the Federal Bureaus of Investigation's Biometric Algorithm Purchase Order Awarded to Idemia National Security Solutions, LLC", Feb. 2022, Department of Justice, Office of the Inspector General, observed June 29th, 2023, at: https://oig.justice.gov/sites/default/files/reports/22-045.pdf, archived at: https://web.archive.org/web/20230629183815/https://oig.justice.gov/sites/default/files/reports/22-045.pdf.

[58] "40 Officers of China's National Police Charged in Transnational Repression Schemes Targeting U.S. Residents", April 17th, 2023, Press Release, US Department of Justice, Office of Public Affairs, observed July 7th, 2023, at: https://www.justice.gov/opa/pr/40-officers-china-s-national-police-charged-transnational-repression-schemes-targeting-us, archived at: https://web.archive.org/web/20230707161909/https://www.justice.gov/opa/pr/40-officers-china-s-national-police-charged-transnational-repression-schemes-targeting-us.

[59] Bowen, Ray, II, "Written Testimony for The United States-China Economic and Security Review Commission (USCC) of the United States Congress For Friday 13 March 2020 Hearing on: A 'China Model?' Beijing's Promotion of Alternative Global Norms and Standards, Panel III: Technological Competition and Driving New Standards, Beijing's Promotion of PRC Technical Standards", March 3rd, 2020, US-China Economic and Security Review Commission, observed July 11th, 2023, at: https://www.uscc.gov/sites/default/files/testimonies/March%2013%20Hearing_Panel%203_Ray%20Bowen%20Pointe%20Bello.pdf, archived at: https://web.archive.org/web/20230711185613/https://www.uscc.gov/sites/default/files/testimonies/March%2013%20Hearing_Panel%203_Ray%20Bowen%20Pointe%20Bello.pdf.

[60] PB Insights, "China Standard 2035: Beijing's plan to dictate global market, IT through standards", posted Dec. 2019, Pointe Bello Official Website, observed July 11th, 2023, at: https://www.pointebello.com/insights/china-standard-2035, archived at: https://web.archive.org/web/20230711190021/https://www.pointebello.com/insights/china-standard-2035.

- Monitor changes in the balance of representation at multilateral standards setting organizations not subject to CPC dominance to increase representation from communities that embrace law to protect individuals.
- Track changes—increases or declines—in CPC-controlled or influenced representation on international standards bodies.
- Gauge growth or attenuation of CPC access to capital—from increase in CPC costs of capital to denial of access to capital markets—for CPC driven technology architectures, hardware, firmware, and software.
- Engage investigators or researchers to identify and call out standards that CPC agents have unduly influenced.
- Map, as a start, relationships of CPC representatives in SAC, CNIS, NCSE, and other CPC-controlled organizations.

A second and higher tier of effort for Congressional legislation to confront PRC standards strategy draws on the moral authority of United States law and our economic might ***to make adherence to global best practices irresistible***. The US commercial and government sectors can improve the use—from conceptualization through implementation—of laws to defend against the CPC's offensive to influence and dominate global standards. The goal should be to create negative consequences for the CPC campaign by implementing laws and policies that focus on the nexus of capability with intent to determine culpability or threat. Specific opportunities for action here include:

- Illuminate the fundamental difference between CPC intent to erect standards that fortify its political position by comparison with Bretton-Woods era derived liberal global institutions' intent to promote prosperity for people. Fundamentally, CPC standards aim to control populations and advance strategic priorities, to include military force projection, rather than "raising productivity, the standard of living, and conditions of labor" globally as the World Bank seeks to do.
- Educate and inform governments, businesses, and populations of the United States and its allies that CPC intent differs widely and deeply in purpose from political parties in constitutionally governed countries and from other participants in standard setting bodies. Standards set by agents primarily under control of the CPC aim to facilitate control, suppression, and containment of populations so that the CPC may protect itself from scrutiny and challenge. A case in point is Beijing's sweeping abuse of technology to control and suppress the PRC's ethnic Uighur population.
- Recognize that the CPC seeks to use courts that it controls to resolve patent dispute matters. The Shenzhen Intermediate People's Court ruled in favor of Huawei and against InterDigital in 2013 regarding the latter's use of its "standards essential patents."
- Conceptually, establish individual liberty and personal security as priorities and basic criteria of foundational intent for acceptance of 5G (and higher) standards for use in the United States. Describe required intent in terms of individual private property rights and human rights.
- Reject 5G (and higher) standards that fail to uphold foundational intent. A 5G standard that the United States rejects cannot be "global."

- Share knowledge of failures to uphold foundationally required intent with U.S. and other legal groups that will follow use of such information to establish culpability or threat— focus on the nexus of capability with intent.
- Map, or catalogue, statements that provide evidence—to a judicial determination level— of PRC intent to abuse standards.

Another realm ripe for action involves the criteria and processes by which standards setting bodies determine who can participate. Frameworks may be strengthened or established to place intent of standards above the specifications those standards establish. Opportunities for action here include:

- Consider requiring nation-of-origin governance-models compatibility—with emphasis on meaningful constitutional governance when deciding which nations' personnel are qualified to participate in standards setting.
- Set criteria to hold any position, including observer, for any standard setting body based on "market economy" country status or, perhaps, based on "freedom" ranking.
- Require participants from non-market economies to provide a credit worthy guarantor or a security guaranty for participating in setting standards, especially for leading standard setting.
- Publish principles to guide setting standards to protect people from states, not to protect states—or political parties—from people. Leverage that distinction to limit the opportunities that CPC leadership can exploit in setting international technical standards, which generally are targeted to provide connectivity to PRC (or PLA) actors.
- Establish criteria to qualify representatives to international standard setting bodies, for example technically qualified individuals from private institutions in market economies can participate in standard setting or technically qualified individuals from legal regimes where all political parties are subject to the same rules in their countries. The CPC applies rules to other political parties in China and to foreign business entities that it does not apply to itself or to businesses it controls.
- Create working groups within NATO and, potentially, other multilateral bodies, to review, modify, or establish standards that affect common concerns.

Bolster Capabilities to Confront and Counter PRC Manipulation of Global Standards Systems

The most forward-leaning tier of effort would attenuate PRC manipulation of global standards systems through measures that impose cost or erode value of standards revised or authored by the CPC; through laws that protect individuals' lives, freedoms, pursuits, and properties; and through actions that engage US allies to suppress the growth of authoritarian control of standard setting bodies. Recognition of PRC operational, practical, or procedural friction areas and how to channel those to support US objectives, and sowing doubt, seeding dilemma, and delaying decision within CPC operational apparatus may also serve to attenuate PRC manipulation. For example:

- Create an "intention trap" that taxes or fines providers of equipment that incorporates or relies upon standards or patents determined to serve intent to protect a government from people, rather than people from government, at rates or with fines in amounts commensurate to the damage determined as the cost to excise and replace offending equipment.

- Build consensus to apply universally accepted non-PRC legal frameworks—e.g., a choice of English, Swedish, or Japanese law—in all dispute resolution and enforcement actions.
- Ensure that the English language is the default and primary controlling language in all standards and patents' legal actions that involve the United States.
- Initiate work - for rapid implementation - with Five Eyes (FVEY) to accept or add processes to accept, reject or propose standards that govern FVEY communities of interest. The first step could be to task a US officer with primary responsibility to identify, monitor and brief each FVEY country on the development of standards according to the criteria discussed here.
- Work with Japan and other Asian communities whose laws protect people from authoritarian governments to roll out and magnify FVEY successes.
- Replicate success from preceding points in Central and South America and Africa.
- Empower insurance underwriters—with combinations of government subsidies, guarantees and requirements—to select US approved or established standards over those set by others. Analogously, US insurers already insist on certain standards—such as requiring fire sprinkler systems in buildings and requiring specific maintenance practices at power plants—before they provide insurance.
- Engage the American National Standards Institute (ANSI) to convene a national task force to examine the "China standards" challenge. ANSI, as the main coordinating body in the United States, is a crossroads for public and private sectors, and is representing US interests in key global standards bodies. Beijing, however, appears to have actively cultivated a relationship with ANSI.
- Require NATO certification to codify certain standards as "complete" and establish a process to certify other standards as perpetually under review or complete only when NATO concurs.
- Implement legal mechanisms to, first, delay accepting, or delay adopting, and then, invalidate standards set with CPC—and therefore by definition with PLA—involvement. US export controls for dual use technologies could serve as drafting model.
- Establish best practices through the procedures described above and promote the reorganization or replacement of existing international standard setting bodies that do not comply with relevant criteria.
- Identify avenues and plan to use those to influence CPC choices of the chairs and committee members of international standards organizations both before and after selection. Publicize evidence of corruption, financial or moral, of individual CPC representatives to standard setting bodies with the objectives of distracting the representatives, enervating their effectiveness, and raising CPC difficulties in staffing standard setting entities.
- Create and deploy the capability of producing regular reports on all CPC designees to standards bodies, not only to identify corruption, but to understand each individual's career path, personal and professional networks, etc. Someone who works at a research institute now may have been seconded from military intelligence last year.