NYU | LAW

Journal of Intellectual Property & Entertainment Law

VOLUME 15 NUMBER 2

Statement of Purpose

Consistent with its unique development, the New York University Journal of Intellectual Property & Entertainment Law (JIPEL) is a nonpartisan periodical specializing in the analysis of timely and cutting-edge topics in the world of intellectual property and entertainment law. As NYU's first online-only journal, JIPEL also provides an opportunity for discourse through comments from all of its readers. There are no subscriptions or subscription fees; in keeping with the open-access and free discourse goals of the students responsible for JIPEL's existence, the content is available for free to anyone interested in intellectual property and entertainment law.

The New York University Journal of Intellectual Property & Entertainment Law is published up to three times per year at the New York University School of Law, 139 MacDougal Street, New York, New York, 10012. In keeping with the Journal's open access and free discourse goals, subscriptions are free of charge and can be accessed via www.jipel.law.nyu.edu. Inquiries may be made via telephone (212-998-6101) or e-mail (submissions.jipel@gmail.com).

The Journal invites authors to submit pieces for publication consideration. Footnotes and citations should follow the rules set forth in the latest edition of The Bluebook: A Uniform System of Citation. All pieces submitted become the property of the Journal. We review submissions through Scholastica (scholasticahq.com) and through e-mail (submissions.jipel@gmail.com).

The Journal is also available on WESTLAW, LEXIS-NEXIS and HeinOnline.

NEW YORK UNIVERSITY

JOURNAL OF INTELLECTUAL PROPERTY AND ENTERTAINMENT LAW

VOLUME 15 SPRING 2026 NUMBER 2

CHIP WALL: CYBERSECURITY CONCERNS WITH THE CHIP SECURITY ACT

WILL SHAO*

Since the COVID-19 pandemic, the world has come to appreciate the critical value of semiconductor chips ("chips"). Countries around the world have prioritized access to these chips in their efforts to improve national and economic security, whether through onshoring chip-making capabilities, forming alliances to share chip-producing resources, or restricting the export of their chips to geopolitical adversaries. The Chip Security Act (CSA) is the most recent legislation proposed in support of such efforts, proposing the implementation of geolocation tracking technologies for covered chips. This note critiques this bipartisan bill, arguing that the CSA may be well-intentioned, but is nevertheless poorly framed. By contextualizing the bill in the broader technical and legal landscape concerning geolocation technologies, it focuses on the ambiguous language and lack of enforcement mechanisms that may not only fail to achieve their security objectives, but also actively harm the U.S. chip industry. By recognizing these issues, I offer several technical and enforcement recommendations to reframe the bill, so that—if enacted—the CSA may provide a nuanced balance between bolstering economic security and protecting against cybersecurity risks.

* J.D. Candidate, New York University School of Law, 2027; M.Sc. in Social Science of the Internet, University of Oxford, 2024. I am incredibly thankful to Professor Judith Germano, whose guidance and support made this note possible. I am also thankful to the Notes Committee of the NYU Journal of Intellectual Property and Entertainment Law for their editorial support, especially Elyse Cox and Jessica Mintz for their exceptionally helpful comments.

Introduction

Semiconductor chips ("chips") are the foundational building blocks of the technological age, powering nearly every electronic device around the world.[1] Major disruptions to the chip supply chain caused by the COVID-19 pandemic underscored their critical importance; factory shutdowns, stay-at-home orders, and other logistical constraints in key chip-producing countries revealed severe bottlenecks that led to widespread chip shortages.[2] Since the pandemic, chips have been at the forefront of national economies worldwide: the U.S. alone exported approximately $56.8 billion in semiconductors in 2024, making it the sixth most exported good by the country.[3] However (and even more importantly), the

[1] Semiconductors are fundamentally materials that can act as both electricity insulators and conductors. These materials are then used to create integrated circuits (otherwise known as chips) capable of performing complicated calculations and storing data. *See* Michael Reid, Falan Yinug, Semiconductor Indus. Ass'n. & Oxford Econ., Chipping In: The Positive Impact of the Semiconductor Industry on the American Workforce and How Federal Industry Incentives Will Increase Domestic Jobs 6 (2021), https://www.semiconductors.org/wp-content/uploads/2021/05/SIA-Impact_May2021-FINAL-May-19-2021_2.pdf [https://perma.cc/VN7A-GE2M]; *see also Semiconductors: Powering the Modern World*, Nat'l Sci. Found., https://www.nsf.gov/impacts/semiconductors [https://perma.cc/3463-26LE] (last accessed Dec. 6, 2025).

[2] *See, e.g.*, Chris Miller, Chip War: The Fight for the World's Most Critical Technology 17-18 (2022) (noting how the pandemic provided "just a glimpse" of how vulnerable the globalized chip supply chain is).

[3] Semiconductor Indus. Ass'n, Semiconductors Power America's Economic Strength, National Security, and Technology Leadership (2026), https://www.semiconductors.org/wp-content/uploads/

revelation of these bottlenecks has since triggered a global race towards economic security in this space. Countries around the world have initiated efforts to reshore their chip-developing capabilities, and—in cases where this is not possible—develop more restrictive alliances to share chip resources.[4] The impacts of such initiatives are even more pronounced for AI-powering chips. As the global race for AI dominance has accelerated since the 2022 launch of ChatGPT, the demand for AI chips has also skyrocketed.[5] Every country hopes to lead (and thereby control) the AI industry, and now both businesses and governments are exploring ways to do so through hardware (including chips) as well as software.

As part of this push for control, several countries have introduced geopolitically-motivated regulations concerning chips.[6] The U.S. specifically has passed several legislations affecting chips, whether we consider the monumental CHIPS and Science Act of 2022 ("CHIPS Act"), or the various export control measures preventing the distribution of leading-edge chips to U.S. adversaries.[7]

2026/03/SIA_StandardIndustry_OnePager_02c48.pdf [https://perma.cc/89LV-APT2]; *see also* Ann Cao, *China's Chip Exports Surge 73% as AI Demand Fuels Semiconductor Growth*, S. China Morning Post (Mar. 10, 2026), https://www.scmp.com/tech/big-tech/article/3346073/chinas-chip-exports-surge-73-ai-demand-fuels-semiconductor-growth [https://perma.cc/D7HZ-GXPC] (providing evidence of how China has similarly increased its export of chips in recent years).

[4] *See, e.g.*, Samer Bahou, Christian G. Dieseldorff & Chih-Wen Liu, *Eighteen New Semiconductor Fabs to Start Construction in 2025, SEMI Reports*, SEMI (Jan. 7, 2025), https://www.semi.org/en/semi-press-release/eighteen-new-semiconductor-fabs-to-start-construction-in-2025-semi-reports [https://perma.cc/E4W6-BA9N] (connecting fab construction trends with growing onshoring and nearshoring priorities); Emily Benson, Japhet Quitzon & William A. Reinsch, *Securing Semiconductor Supply Chains in the Indo-Pacific Economic Framework for Prosperity*, Ctr. for Strategic & Int'l Stud., (May 30, 2023), https://www.csis.org/analysis/securing-semiconductor-supply-chains-indo-pacific-economic-framework-prosperity [https://perma.cc/7HGA-ZJHB] (exploring alternative chip partners to China in the Indo-Pacific for the U.S.).

[5] *See* Ondrej Burkacky et al., *Generative AI: The Next S-curve for the Semiconductor Industry?*, McKinsey & Co. (2024), https://www.mckinsey.com/industries/semiconductors/our-insights/generative-ai-the-next-s-curve-for-the-semiconductor-industry#/ [https://perma.cc/N5HS-AJUC].

[6] *See* Jason Wilcox, *U.S. AI Chip Policy: A Post-Recission Forecast*, Baker Botts (July 23, 2025), https://www.bakerbotts.com/thought-leadership/publications/2025/july/us-ai-chip-policy [https://perma.cc/3PDN-3LT9] (addressing more recent trends in U.S. chip policy under the Trump Administration); *see also* Mary Thornton, *The Critical Effort to Combat Illicit Chip Diversion*, Semiconductor Indus. Ass'n (Oct. 11, 2024), https://www.semiconductors.org/the-critical-effort-to-combat-illicit-chip-diversion/ [https://perma.cc/26N5-P9GQ] (acknowledging industry-driven initiatives to adhere to national policies on chip exports).

[7] *See, e.g.*, CHIPS and Science Act of 2022, Pub. L. No. 117-167, 136 Stat. 1366 (2022); Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items;

The Chip Security Act (H.R.3447/S.1705, later referred to as "the CSA") is the most recent iteration of such regulations. This bipartisan bill was proposed on May 15, 2025, and has been referred to the House Committee on Foreign Affairs at the time of writing.[8] Its main purpose is to further support export control efforts by enabling geolocation tracking of covered chips.[9] While the bill's purpose is understandable in our current geopolitical climate, its execution is heavily misguided.[10] Its ambiguous language and lack of enforcement mechanisms expose it to various challenges, particularly in the cybersecurity space. Therefore, this note argues that the CSA in its current form is well-intentioned but poorly framed, opening up the possibility for this legislation to not only fail to achieve its objectives, but also harm the U.S. economy and national security.

This note will proceed as follows. After providing an overview of the CSA and its main provisions, the note surveys the current technical landscape of geolocation technologies. By highlighting the cybersecurity weaknesses they face, it demonstrates how enforcing the bill's provisions as they currently exist may result in serious harm for the U.S. chip industry. The note then turns its attention towards the U.S. legislative landscape pertaining to chips. While there are many instances in which legislations complement each other and provide a more holistic approach to chip regulation, there are also several key issues they fail to address collectively. Finally, this note brings these critiques together to propose certain amendments to the CSA. By including both technical and enforcement-related revisions, it hopes to provide a means for the CSA—if enacted—to valuably contribute to the U.S. legal landscape on export controls.

Supercomputer and Semiconductor End Use; Entity List Modification, 87 Fed. Reg. 62186, 62188–9 (Oct. 13, 2022). *See also* No Advanced Chips for the CCP Act of 2025, H.R. 5022, 119th Cong. (2025) (a more recent proposal for chip exports specifically targeting the CCP).

[8] *See* Actions on H.R. 3447, 119th Cong. (2025), https://www.congress.gov/bill/119th-congress/house-bill/3447/all-actions [https://perma.cc/3538-DSHB]

[9] H.R. 3447, 119th Cong. § 2(4)–(5) (2025) (proclaiming how geolocation-driven chip security mechanisms can improve compliance with export controls, help detect smuggling, and streamline the legitimate exports of chips).

[10] *See* Paul Lekas, *The Chip Security Act is the Wrong Approach to Preventing Chip Diversion*, Software & Info. Indus. Ass'n, (July 25, 2025), https://www.siia.net/the-chip-security-act-is-the-wrong-approach-to-preventing-chip-diversion/ [https://perma.cc/Q6NN-KDQF] (commenting that the proposal is simply seeking "an easy solution to a complex problem").

I
The Chip Security Act: An Overview

The CSA has two broad objectives. First, it seeks to capitalize on the security and economic benefits of U.S.-developed AI chips, constraining such benefits to "the United States and allies and partners of the United States".[11] Second, it aims to strengthen existing export controls by preventing the "diversion, theft, and other unauthorized use or exploitation" of those chips by adversaries, thereby maintaining U.S. national security and technological competitiveness.[12] To achieve these goals, the CSA would require that "any covered integrated circuit product [must be] outfitted with chip security mechanisms that implement location verification, using techniques that are *feasible and appropriate on such date of enactment*, before it is exported, reexported, or in-country transferred to or in a foreign country" (emphasis added).[13] Credible information about a chip's location that does not conform to its license or authorization must be reported to the Under Secretary of Industry and Security.[14]

The bill includes two additional provisions related to these requirements. First, chip security mechanisms are broadly defined to include "software-, firmware-, or hardware-enabled security mechanism[s] or a physical security mechanism."[15] Second, as the entity responsible for enforcing the CSA, the Secretary of Commerce ("the Secretary") must conduct post-enactment assessments to identify additional security mechanisms to add or replace existing ones.[16] These assessments must account for the feasibility, reliability, effectiveness, cost, and vulnerabilities of such additions.[17]

The Secretary has three other responsibilities of particular relevance to this note. First, the Secretary may maintain "a record of covered integrated circuit products and include in the record the location and current end-user of each such product".[18] This is relevant insofar as various scholars have proposed the creation

[11] H.R. 3447 § 2(1).
[12] *Id.* § 2(3).
[13] *Id.* § 4(a)(1).
[14] *Id.* § 4(a)(2).
[15] *Id.* § 3(2).
[16] *Id.* § 4(b)(1)(A).
[17] *Id.* § 4(b)(1)(B).
[18] *Id.* § 4(c)(2).

of a chip registry.[19] Second, the Secretary may also verify "in a manner the Secretary determines appropriate" the ownership and location of a chip.[20] Third, the Act provides a cursory acknowledgement of cybersecurity concerns, stating that in "implementing requirements for secondary chip security mechanisms […], the Secretary shall prioritize confidentiality".[21]

II
Chip Geolocation: The Technical Landscape

As noted above, the CSA requires that covered chips be fitted with geolocation mechanisms which use "techniques that are *feasible and appropriate on such date of enactment*" (emphasis added).[22] The broad language of the bill offers the advantage of flexibly accommodating future technological innovations. However, presuming the CSA is enacted before new geolocation technologies are commercially available, this ambiguity raises a host of cybersecurity issues. Current mechanisms, while in certain cases beneficial, have a well-documented history of security vulnerabilities that could operate against the fundamental goals of this bill. The following section focuses on these technical issues, highlighting how geolocation technologies across three categories—asset-reported, topology-based, and delay-based—could cause greater harm than good if implemented as per the requirements of the CSA.

A. Asset-Reported

Asset-reported geolocation requires the asset (in this case, the chip) to use external signals to calculate its location.[23] The asset then reports that location to a trusted server for verification.[24] The most common example of this is GPS: a

[19] *See, e.g.*, Asher Brass & Onni Aarne, Location Verification for AI Chips 29 (2024) https://static1.squarespace.com/static/64edf8e7f2b10d716b5ba0e1/t/6670467ebe2a477eb1554f40/1718634112482/Location%2BVerification%2Bfor%2BAI%2BChips.pdf [https://perma.cc/RP98-7DPB]; Erich Grunewald & Michael Aird, AI Chip Smuggling into China: Potential Paths, Quantities, and Countermeasures 59-61 (2023), https://static1.squarespace.com/static/64edf8e7f2b10d716b5ba0e1/t/651bb8a18f961e3333e3c1d7/1696315558319/AI+chip+smuggling+into+China+%5Bfinal%5D.pdf [https://perma.cc/7669-QJ2F].

[20] H.R. 3447 § 4(c)(1).

[21] *Id.* § 4(b)(3)(B).

[22] *Id.* § 4(a)(1).

[23] *See* Brass & Aarne, *supra* note 19, at 13.

[24] *Id.*

receiver on the ground receives navigation messages from at least four orbiting satellites, each containing the precise time of transmission.[25] The receiver can then calculate its distance in relation to each satellite, thereby estimating its own location through multilateration.[26] As may be obvious by its pervasive use, GPS tracking is very well understood at the technical level.[27] Furthermore, it is extremely precise; studies have shown that under optimal conditions, GPS and similar asset-reported technologies have an accuracy range roughly between 3 to 100 meters.[28]

However, asset-reported technologies are also notorious for their cybersecurity vulnerabilities.[29] Most notably, civilian GPS systems are highly vulnerable to spoofing attacks. By recording legitimate radio signals, an attacker can replay identical—but higher power—signals in order to provide a false location or cause a receiver to lock onto the spoofing signal instead (i.e., a seamless satellite-lock takeover).[30] This is achievable because civilian GPS systems are typically unencrypted and insecure, which allows even unsophisticated adversaries to easily launch spoofing attacks at minimal cost.[31] Technical mechanisms do exist to mitigate the spoofability of GPS and asset-reported systems. Auxiliary peak tracking (APT) is one such example, providing the ability to counter seamless takeover attacks and limit spoofability of an asset's location to a one-kilometer radius.[32] However, the efficacy of such techniques remains limited by the fact that commercially-available chips—even those equipped with on-chip governance

[25] Aanjhan Ranganathan, Hildur Ólafsdóttir & Srdjan Capkun, *SPREE: A Spoofing Resistant GPS Receiver*, ArXiv (Mar. 17, 2016), https://arxiv.org/abs/1603.05462 [https://perma.cc/PTV6-HUSZ].

[26] *Id.*

[27] *See* Brass & Aarne, *supra* note 19, at 5.

[28] *See id.* at 4.

[29] *See id.* at 5 (noting how asset-reported methods have a history of manipulation by adversaries).

[30] *See, e.g.,* Ranganathan, Ólafsdóttir & Capkun, *supra* note 25, at 3-5 (overviewing various types of GPS spoofing attacks, as well as discussing seamless lock takeover); Nils O. Tippenhauer et al., *On the Requirements for Successful GPS Spoofing Attacks*, Proc. of the 18th ACM Conf. on Comput. & Commc'ns Sec. 75, 81-82 (2011) (providing sample ranges for signal power, constant time offset, location offset, and relative time offset to achieve a seamless lock takeover in their experiment).

[31] *See* Brass & Aarne, *supra* note 19, at 5 (estimating a cost of roughly $200 to spoof a GPS system). *See also* Ranganathan, Ólafsdóttir & Capkun, *supra* note 25, at 3 (noting how an attacker's spoofing signal can "trivially overshadow" the lower power of a legitimate satellite signal).

[32] *See* Ranganathan, Ólafsdóttir & Capkun, *supra* note 25, at 5, 9 (Fig. 9).

mechanisms—are not yet designed to protect against actors with physical access to them, let alone against those with a lot of resources at their disposal.[33]

An obvious consequence of this vulnerability is that mandating asset-reported systems could do little to restrict the illegitimate export of chips. Especially given that well-resourced actors can currently bypass the security measures of current on-chip governance mechanisms, these systems may give a false sense of security: the government may believe it can readily track U.S.-developed chips, all while their locations are actually being spoofed. There are two additional consequences to note. First, spoofing attacks can sometimes cause permanent damage to receivers.[34] This should raise concerns about such attacks dismantling underlying infrastructures and in turn resulting in further loss of chips. Second, installing asset-reported mechanisms would create a digital, trackable footprint for each chip.[35] With enough targeted attacks, adversarial actors could access the location data of chips used in sensitive systems across the U.S. and abroad.[36] Thus, while asset-reported mechanisms would provide the American government with greater transparency about chip locations, it could also give a similar amount of visibility to its adversaries.

Another critical issue with asset-reported mechanisms concerns their reliability. As mentioned above, GPS systems are highly accurate and precise. However, such precision requires unobstructed signals from satellites.[37] As such, GPS systems do not work well with tracking assets in indoor environments, which

[33] *See, e.g.*, Onni Aarne, Tim Fist & Caleb Withers, Secure, Governable Chips: Using On-Chip Mechanisms to Manage National Security Risks from AI & Advanced Computing 2 (2024), https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS-Report-Tech-Secure-Chips-Jan-24-finalb.pdf [https://perma.cc/QY4D-KKP7] (acknowledging this limitation as it applies to on-chip governance mechanisms more broadly). *But see* Ranganathan, Ólafsdóttir & Capkun, *supra* note 25, at 11–12 (providing technical recommendations for how to integrate SPREE into a modern GPS receiver with minimal complications).

[34] Ranganathan, Ólafsdóttir & Capkun, *supra* note 25, at 4.

[35] *See* Joseph Hoefer, *Why Tracking The Location Of AI Chips Is a Mirage — and a Risk*, Tech Pol'y.Press (May 23, 2025), https://www.techpolicy.press/why-tracking-the-location-of-ai-chips-is-a-mirage-and-a-risk/ [https://perma.cc/AML5-YE7E] (noting how tracking systems on chips will more likely broadcast sensitive locations of chips than protect them).

[36] *See id.*

[37] Fahim Ahmed et al., *Comparative Study of Asset Location and Tracking*, 51 Procedia Mfg. 1138, 1139 (2020) (explaining that GNSS systems—among which GPS is a U.S.-owned constellation—do not work indoors because there is "no direct line-of-sight between the antenna and satellites").

will often be the case with data centers potentially containing illicitly exported chips.[38] There are alternative asset-reported mechanisms that are better suited to indoor tracking, such as ultra-wide band and radio-frequency identification.[39] However, these require additional reference points like beacons or anchors to help triangulate an asset's location.[40] Given that using such systems would require additional infrastructure, it is unlikely that they could be successfully adopted prior to the enactment of this bill (at least, in an idealized timeline).[41] Therefore, asset-reported mechanisms not only introduce a number of spoofing and cybersecurity concerns, but they may also not be effective in the near future given current technical and infrastructural limitations.

B. Topology-Based

Topology-based geolocation relies on the asset reporting measurements of radio-frequency emitters within its range and widely deployed in the target region.[42] These frequencies may originate from cell towers, Wi-Fi routers, or similar radio frequency beacons, to name a few.[43] By combining those measurements with information about both the known locations of the emitters (typically acquired from public Whois databases, DNS records, or other infrastructures) and the asset's digital characteristics (such as an IP address or Wi-Fi SSID), one can calculate the location of a given asset.[44] Network-based mobile phone tracking and geolocalization from an IP address are two common use cases of topology-based mechanisms.[45] In addition to their efficiency advantage of relying on existing digital infrastructure, these mechanisms are also highly accurate. In certain cases, they maintain a margin of error between 50 to 500 meters.[46] Topology-aware methods even go a step further, incorporating round-

[38] Brass & Aarne, *supra* note 19, at 5.

[39] Ahmed et al., *supra* note 37, at 1140.

[40] *Id.* at 1142-3 (describing how beacons and tags are necessary to assist with Bluetooth tracking indoors).

[41] *See generally id.* at 1143 (noting that the infrastructure for Bluetooth-powered tracking does not yet exist and would be very costly to set up to ensure good signal).

[42] Brass & Aarne, *supra* note 19, at 4.

[43] *Id.*

[44] *See, e.g.*, Brass & Aarne, *supra* note 19, at 15; Philippa Gill et al., *Dude, Where's That IP? Circumventing Measurement-Based IP Geolocation*, in *Procs. of the 19th USENIX Sec. Symposium*, at 2 (2010) (highlighting the potential use of proprietary or public databases of IP for location mappings).

[45] Brass & Aarne, *supra* note 19, at 15.

[46] *Id.* at 4.

trip time (RTT) measurements and network topology data to further increase their accuracy.[47]

However, much like asset-reported mechanisms, topology-based methods are highly prone to cybersecurity threats. To start, these mechanisms may also be easily spoofed: attackers can either reroute geolocation pings through proxy networks, or simply disable the pings entirely.[48] The level of ease is due to these mechanisms relying on protocols and infrastructures (such as DNS) considered insecure against technologically advanced actors.[49] As a result, many of these topology-based methods have long been victims of adversarial attacks.[50] Additionally, the reliance of these mechanisms on publicly available databases introduces another cybersecurity concern through presenting a new angle for corruption by third parties.[51] A similar issue arises for systems that rely on submitted data (like HTTP headers) that could easily be falsified.[52] Thus, perhaps even more so than asset-reported systems, there are several ways in which topology-based mechanisms may be manipulated.

In addition to how easy such corruption can technically be, it is more concerning how subtly it can happen in comparison to asset-reported mechanisms. For example, sophisticated adversaries like Infrastructure as a Service (IaaS) providers may capitalize on their control over multiple network entry points to attack a geolocation system.[53] Not only does this technique return a high-accuracy forged result, but it is also much harder to detect using common metrics like region size.[54] In addition, the highly-accurate topology-aware techniques mentioned above may actually face a higher likelihood of covert tampering because of the increased number of inputs one may manipulate (such as traceroute data and undns entries).[55] Thus, mandating the use of such geolocation mechanisms could in fact

[47] Gill et al., *supra* note 44, at 2.

[48] *See* Hoefer, *supra* note 35.

[49] Brass & Aarne, *supra* note 19, at 15.

[50] *Id.*

[51] Gill et al., *supra* note 44, at 11 (highlighting the possibility of database poisoning when geolocation relies on *undns*).

[52] *See* Christian Esposito et al., *On Data Sovereignty in Cloud-Based Computation Offloading for Smart Cities Applications*, 6.3 IEEE Internet of Things J. 4521, 4525 (2019).

[53] Gill et al., *supra* note 44, at 15.

[54] *Id.*

[55] *Id.*

result in greater adoption of these manipulation tactics that do little to improve the current export control situation.

Finally, topology-based mechanisms typically require the addition of physical components (at the very minimum, an antenna to the die) to an asset for geolocation purposes.[56] Much like with receivers in asset-reported mechanisms, this addition provides another, physical avenue for adversarial actors to launch cyberattacks against covered chips more easily. Studies have already explored the various types of physical attacks adversaries may use, ranging from fully-invasive modifications to side-channel analysis attacks.[57] Furthermore, the addition of physical components may be technically infeasible, if not at the very least burdensome. This is particularly the case for chips, given their already-extreme compactness.[58] Therefore, topology-based geolocation mechanisms are not only easily spoofable and harder to detect, but they may also impose additional requirements on manufacturers that are too technically challenging to be economically viable.

C. Delay-Based

The final category—delay-based geolocation—is considered the most technically relevant of the three.[59] It works by requiring a cryptographic challenge-response between the asset and a landmark or series of landmarks (servers in known locations).[60] Once the asset sends a ping to the landmark, the RTT is used to determine the maximum possible distance the transmission could have traveled and the asset's location by proxy.[61] There are two key components to keep in

[56] Brass & Aarne, *supra* note 19, at 5.

[57] *See* Gabriel Kulp et al., *Hardware-Enabled Governance Mechanisms: Developing Technical Solutions to Exempt Items Otherwise Classified Under Export Control Classification Numbers 3A090 and 4A090*, 22-25 (RAND Corp., Working Paper No. WR-A3056-1, 2024), https://www.rand.org/pubs/working_papers/WRA3056-1.html [https://perma.cc/Y6R6-8UYV] (describing both physical and nonphysical attack vectors that adversaries could pursue).

[58] *The Basics of Microchips*, ASML, https://www.asml.com/en/technology/all-about-microchips/microchip-basics, (last visited Apr. 14, 2026) (noting how some features in the most advanced microchips are merely a few dozen nanometers in size).

[59] *See* Brass & Aarne, *supra* note 19, at 6 (indicating such relevance stems from its encrypted communication and "relative lack of reliance on public infrastructure", thereby enhancing certain security features).

[60] *See, e.g.,* Brass & Aarne, *supra* note 19, at 15.

[61] *Id.*; *see also* Aidan O'Gara et al., Hardware-Enabled Mechanisms for Verifying Responsible AI Development 14 (2025) (unpublished manuscript), arXiv:2505.03742.

mind for delay-based mechanisms: (1) the delays combine with multilateration to help determine the maximum possible distance; and (2) such techniques often use a cryptographic proof of identity, such as a Trusted Platform Model (TPM) that protects a unique secret key specific to a chip.[62]

Delay-based mechanisms offer a host of benefits not provided by the other two categories. For starters, they place emphasis on system security and are in turn considered more difficult to spoof and falsify.[63] On a similar note, these mechanisms are considered privacy-oriented and nonintrusive given their capabilities to confirm a chip's location without overbearing surveillance.[64] In addition, given that such solutions are primarily software-based, they are easier and relatively cheap to implement.[65] This makes them an appealing option for short-term adoption, as well as longer-term maintenance given the ease of updating them. Finally, although it is not necessarily as precise as the other two options, delay-based geolocation is considered sufficiently precise for export control enforcement, establishing an upper bound on the distance and being capable of providing clear evidence for whether a chip is in restricted territory.[66]

However, as much of an improvement as this mechanism seems to be from a cybersecurity lens, delay-based methods still pose notable threats. First, while traditional spoofing is harder to achieve given the cryptographic security measures, it is not impossible if an adversary discovers and copies the secret private key.[67] That being said, an adversary may not even need to do that to achieve spoofing-like effects; one may still be able to manipulate the response times to alter a chip's perceived location without the key.[68] For instance, adversaries may use dark fiber,

---

[62] *See* Esposito, *supra* note 52, at 4525. *See also* Brass & Aarne, *supra* note 19, at 20.

[63] *Id.* at 1.

[64] *See, e.g.,* Kit Conklin, *How the Chip Security Act Could Usher in an Era of 'Trusted Trade' with US Partners*, Atl. Council (Aug. 18, 2025), https://www.atlanticcouncil.org/blogs/geotech-cues/how-the-chip-security-act-could-usher-in-an-era-of-trusted-trade-with-us-partners/ [https://perma.cc/6UPA-ABNH]; Tim Fist, Tao Burga & Vivek Chilukuri, Technology to Secure the AI Chip Supply Chain: A Working Paper (2024), https://www.cnas.org/publications/reports/technology-to-secure-the-ai-chip-supply-chain-a-primer [https://perma.cc/U6LD-RKNB] (including delay-based mechanisms under the broad heading of HEMs).

[65] *See* Fist, Burga & Chilukuri, *supra* note 64.

[66] Brass & Aarne, *supra* note 19, at 1.

[67] O'Gara et al., *supra* note 61, at 15 (noting how transferring the cryptographic key could undermine the entire cryptographic protocol).

[68] *Id.*

private terrestrial connections, or quicker out-of-band communication methods to trigger faster response times that make a chip appear closer to a landmark.[69] On the opposite end of the spectrum, such actors may want to deliberately slow down the transmission to increase the potential region size for the chip's location. This may in turn cause a party to have growing uncertainty about the geolocation estimation, and perhaps even distrust its measurements to the tracker's detriment.[70] Thus, there are several technical means that have a spoofing effect and may reduce the efficacy of delay-based geolocation.

Second, the external landmark servers themselves are vulnerable to direct attacks. Such attacks can be both physical and digital. To start with the former, landmarks placed within striking distance of an adversary are at increased risk of a malicious takeover through cyber-physical means.[71] As for the latter, landmarks may be subject to distributed denial of service (DDoS) attacks on their clock or timestamp systems, which could in turn cause them to misreport the RTT.[72] As such, landmark servers function as another avenue for adversaries to launch attacks against these geolocation systems, either through overloading their network traffic or attacking the physical landmark itself. Therefore, while it is certainly the most promising approach of the three for balancing economic security and cybersecurity concerns, delay-based mechanisms still pose several significant cybersecurity challenges that complicate their adoption, whether on account of an adversary's ability to manipulate response times or through introducing a new physical vulnerability.

III
Chip Geolocation: The Legal Landscape

The CSA not only raises several technical issues, but it also provides minimal novel value from a legal standpoint. The text itself is incredibly sparse. For starters, it mandates the implementation of location verification on chips without discussing how it would actually enforce compliance. The closest we get to that information is a vague statement that the Secretary *may* verify "in a manner the Secretary

[69] *See id.*; *see also* Brass & Aarne, *supra* note 19, at 6.

[70] Brass & Aarne, *supra* note 19, at 22. *See also* Gill et al., *supra* note 44, at 7–8 (discussing the technical means of increasing the reported region size of delay-based mechanisms).

[71] O'Gara ext al., *supra* note 61, at 15.

[72] *See id.; see also* Brass & Aarne, *supra* note 19, at 26.

determines appropriate" the location of a covered chip, and *may* maintain a record of covered chips.[73] Additionally, the bill provides a notification requirement for those who identify violations of the Act, but provides no insights into what sanctions or repercussions noncompliant actors might face.[74] There is arguably some value to the Secretary reports mandated by the bill, given the importance of keeping abreast with recent technological developments in the industry. However, beyond this, the bill provides little guidance on how it intends to actually remedy the export control situation.

As such, this section turns to current legislative and regulatory initiatives that impact the export or geolocation of chips. In providing an overview of their scope, gaps, and overall effectiveness, this section achieves two objectives. First, it will demonstrate ways in which the CSA builds on existing regulatory initiatives. Second, it will highlight potential opportunities for a redrafting of the CSA to tackle these geolocation issues from a novel angle.

A. Export Control Reform Act (ECRA)

The ECRA is a federal statute that imposes and enforces export controls on technological assets, including AI-powering chips.[75] As part of this statute, the Secretary of Commerce must maintain a list of controlled items, foreign persons and end users that pose a threat to U.S. national security and foreign policy.[76] Additionally, the Secretary must "establish a procedure to license or otherwise authorize the export, reexport, and in-country transfer of" controlled goods.[77] Finally, the Bureau of Industry and Security (BIS) has released several Interim Final Rules (IFRs) regarding the ECRA and advanced chips, setting detailed parameters to ensure chip movement is controlled. The most notable rules are ECCN 3A090 and 4A090, which collectively control advanced computing chips and technologies containing them, with the goal of preventing their proliferation and minimizing the risk of their misuse in training AI systems.[78]

---

[73] H.R. 3447, 119th Cong. § 4(c)(1)-(2) (2025).

[74] *Id.* at § 4(a)(2).

[75] Export Control Reform Act, 50 U.S.C. §§ 4801–4852 (2018).

[76] *Id.* at § 4813(a)(1)–(2).

[77] *Id.* at § 4815(a).

[78] Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items; Supercomputer and Semiconductor End Use; Entity List Modification, *supra* note 7, at 62188-9.

The ECRA is perhaps the most relevant legislation to the CSA due to the fact it is referenced at multiple points throughout the CSA, either to provide certain key definitions, or to clarify the scope of those who are required to notify the Secretary of violations.[79] The framing of the CSA likely seeks to address the noncompliance issues the ECRA has faced, as there has been a history of pervasive AI chip smuggling since its enactment.[80] Additionally, mandating geolocation tracking in the CSA attempts to resolve the lack of post-export visibility mechanisms that plagued the ECRA.[81] The ECRA also fills a number of gaps that are not addressed by the CSA. For starters, it provides a criminal penalty against those who *willfully* commit a violation.[82] Furthermore, the ECRA requires exporters to conduct due diligence in their operations, including reviewing publicly available information and market data.[83]

However, there are notable gaps and issues that neither legislation addresses in their current forms. For starters, the mens rea requirement for a criminal violation under the ECRA may inappropriately incentivize a company to only perform the minimum due diligence required to avoid legal exposure.[84] The complete lack of any reference to this in the CSA means this remains a significant issue. Additionally, the efficacy of enforcing the ECRA is largely dependent on the BIS budget, one that has majorly decreased over the past few years despite a substantial increase in its responsibilities.[85] Such resource constraints in turn mean that the BIS have limited capacity to deal with smuggling cases. The CSA merely exacerbates this issue by placing additional requirements on the Department of Commerce to fulfill. Thus,

[79] H.R. 3447, 119th Cong. §§3(4)-(6), 4(a)(2) (2025).

[80] Erich Grunewald & Tim Fist, Countering AI Chip Smuggling Has Become a National Security Priority: An Updated Playbook for Preventing AI Chip Smuggling to the PRC 5 (2025), https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/Countering-AI-Chip-Smuggling-Has-Become-a-National-Security-Priority-CNAS-Working-Paper-2020-format_061125_Final.pdf [https://perma.cc/5CLU-GUTD] (exploring this in the specific context of the PRC).

[81] *See Congress Considers Legislation to Shift Export Control Jurisdiction from the Department of Commerce*, Morgan Lewis, https://www.morganlewis.com/pubs/2022/11/congress-considers-legislation-to-shift-export-control-jurisdiction-from-the-department-of-commerce [https://perma.cc/NVA8-C5PS] (Nov. 7, 2022) (noting the Department of Commerce's and the BIS's lack of success in tightening restrictions).

[82] 50 U.S.C. §4843(a) (2018).

[83] Implementation of Additional Export Controls: Certain Advanced Computing Items: Supercomputer and Semiconductor End Use; Updates and Corrections, 88 Fed. Reg. 73458, 73468 (Nov. 17, 2023).

[84] Grunewald & Fist, *supra* note 80, at 8.

[85] Grunewald & Aird, *supra* note 19, at 16.

while the combination of these bills provides sanctions and punishments against those who violate export controls, they still leave important questions around accountability and enforceability unanswered.

B. 18 U.S.C. § 1030: Computer Fraud and Abuse Act (CFAA)

The CFAA is a criminal statute that primarily targets computer crime. At its core, it prohibits someone from accessing a computer "*without authorization* or *exceed[ing] authorized access*" to obtain information (emphasis added).[86] The recent *Van Buren* decision further clarifies the scope of 'exceeding authorized access', providing a gates-up-or-down framework that limits the inquiry to whether someone had the right to access the computer in the first place.[87] While the statute does not explicitly refer to or cover semiconductors, its definitions of "computer" and "protected computers" are broad enough to potentially include these chips (at least in certain circumstances).[88] Admittedly, chips themselves are not "information", which appears to be what the statute is primarily aimed to cover. However, one could argue that their use in training information-generating AI models—and potentially to the detriment of U.S. national security and foreign relations—is sufficient evidence that they should be covered by this statute.[89]

Extending the CFAA to cover chips would arguably be beneficial in providing an additional legal means to pursue liability (one with clearly dictated penalties no less).[90] The geolocation requirements of the CSA may also help with the enforcement of the CFAA in such situations, as the government could identify violating parties and hold them accountable through both economic sanctions and criminal penalties under this statute (jurisdiction-depending) more readily. That being said, one potential issue that this strategy may face concerns the focus on unauthorized "access" as opposed to "misuse".[91] If, in a hypothetical scenario, legitimate access is gained to a covered chip, then the CFAA would be rendered irrelevant even if there is potential misuse of the chips. This is significant given the

[86] Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (a)(2).

[87] Van Buren v. United States, 593 U.S. 374, 396 (2021). *See also* Orin Kerr, *The Supreme Court Reins in the CFAA in Van Buren*, Lawfare (June 9, 2021), https://www.lawfaremedia.org/article/supreme-court-reins-cfaa-van-buren [https://perma.cc/YT7A-JSXG].

[88] 18 U.S.C. §1030(e)(1)–(2).

[89] *Id.* §1030(c)(4)(A)(i)(V).

[90] *Id.* §1030(c).

[91] *Van Buren*, 593 U.S. at 403.

White House's recently-introduced policy of allowing certain chip exports to China for receiving a percentage of the revenue.[92] Therefore, the CFAA could provide more robust legal structures to protect U.S.-developed chips, but only in specific circumstances.

C. CHIPS Act

The CHIPS and Science Act is the final major legislation relating to the security and export of chips.[93] Enacted in 2022, the Act allocated $52.7 billion to revitalize the semiconductor industry in the U.S. and secure its supply chain through supporting R&D, manufacturing, and workforce development.[94] The CHIPS for America Fund then allocated $39 billion to incentivize investment in facilities for chip fabrication, assembly, testing, and packaging.[95] While the CHIPS Act and the CSA are both motivated by national security and economic security objectives, they aim to achieve those goals in two distinct ways: the former seeks to build up resiliency by investing in the domestic supply chain, while the latter seeks to cement U.S. technological leadership through restraining the dissemination of its chips.

The CHIPS Act admittedly has little to do with the enforcement of export controls on existing chips, focusing much more on promoting specific industry policies. However, government-driven funding allocation may be critical in supporting both innovation in geolocation technologies, and enforcement initiatives by regulatory bodies like BIS. Both factors would be core to ensuring the success of the CSA, and neither are addressed at all in the text of the bill. Therefore, putting aside the critiques that the CHIPS Act has received from the international sphere,[96] the questions around funding allocation from the CHIPS Act may be critical in determining the long-term efficacy of the proposed CSA.

---

[92] Lily Jamali & Osmond Chia, *Trump Gives Nvidia Green Light to Sell Advanced AI Chips to China*, BBC (Dec. 8, 2025), https://www.bbc.com/news/articles/ckg9q635q6po [https://perma.cc/MP7J-DGXU].

[93] CHIPS and Science Act of 2022, *supra* note 7.

[94] "Mark" Min Seong Kim, *Chip Security: Reconciling Industrial Subsidies with WTO Rules and National Security Exception*, 16 HARV. NAT'L SEC. J. 74, 76 (2025).

[95] *Id.* at 94.

[96] *Id.* at 78 (noting how countries like China had raised trade complaints against these subsidies at the WTO).

IV
A Revised CSA: Technical and Enforcement Recommendations

As the above discussion has hopefully shown, the CSA may be well-intentioned but poorly executed. On the technical front, its mandates do not consider the limitations and vulnerabilities of current geolocation technologies, thereby potentially exposing chips to a wide variety of cybersecurity risks. On the legal front, it provides little guidance on enforcement or penalties, leaving existing statutes to (imperfectly) fill in the gaps where possible. However, the CSA need not be so passive in its legislative contributions. In light of the issues raised above, this note provides critical recommendations for how we may revise the CSA. These recommendations—organized into two overarching categories—seek to enhance cybersecurity protections for covered chips, while also retaining the economic security spirit that initially drove this proposal.

A. Technical Recommendations

There are several ways in which the CSA could be revised to provide chips with stronger cybersecurity protections. Perhaps the easiest and most immediately enforceable change could be a mandate to use technologies whose geolocation mechanisms are at least as sophisticated as delay-based ones, if not more so. As already mentioned, delay-based options offer the most robust security among the mechanisms currently available.[97] Furthermore, given they are primarily software-based, delay-based options are not only easily implementable, but also are more suited to longer-term sustainability through updates.[98] Some experts have noted that there are certain instances in which the other two methods may serve as sufficient deterrence against malicious actors, thereby providing what companies might see as more cost-effective alternatives.[99] However, this should be considered an exception more so than a norm; while the initial set-up and maintenance costs for delay-based mechanisms may be higher, their stronger security measures should be considered a valid investment in better ensuring economic and national security.

This type of legal formulation is not without its precedents. For example, the IoT Cybersecurity Improvement Act of 2020 notes that the Director of NIST

[97] Brass & Aarne, *supra* note 19, at 6.

[98] O'Gara et al., *supra* note 61, at 7.

[99] *See* Brass & Aarne, *supra* note 19, at 6 (noting how current asset-based and topology-based methods could be secure enough if an adversary is "very worried about being caught").

must establish a series of guidelines and standards on appropriate agency use of IoT devices, including "minimum information security requirements for managing cybersecurity risks associated with such devices".[100] While not as explicit as mandating a specific kind of technology as the baseline, it does require a more active setting of a baseline than what the CSA currently offers. Furthermore, the IoT Act provides exceptions to the prohibition of IoT devices that do not meet such minimum requirements in the case of national security, necessity for research purposes, or the existence of alternative and effective security methods.[101] This demonstrates the recognition that governments are aware of exceptional circumstances that may warrant different treatment, but nevertheless still opt to establish a baseline minimum security standard as I have proposed for the CSA. Therefore, rather than vague phrasing of "feasible and appropriate on such date of enactment",[102] the statute could instead mandate by default an adoption of delay-based geolocation mechanisms. As an exception, the CSA could allow a chip provider to offer in writing a sufficient reason for why one of the current alternative methods should be adopted for their product.

In addition, the CSA could require that geolocation capabilities be fitted with tamper-proof and tamper-evident systems, both of which would provide further layers of security. This technology is already available in certain contexts, especially if the above recommendation for a delay-based mechanism default is adopted (given their reliance on cryptographic identity proofs like TPMs).[103] Furthermore, proposing the adoption of additional security measures is not legally unheard of, as best demonstrated by the mandated shift towards Zero Trust Architecture in federal information systems by Executive Order 14028.[104] For the purposes of the CSA, An additional security step could be to use threshold cryptography, which involves splitting the storage of keys across several separate

[100] Internet of Things Cybersecurity Improvement Act of 2020, Pub. L. No. 116-207, 134 Stat. 1002, §4(a)(1) (2020).

[101] *Id.* §7(b)(1).

[102] H.R. 3447, 119th Cong. §4(a)(1) (2025).

[103] *See* Nat'l Inst. of Standards & Tech., *Sec. Requirements for Cryptographic Modules*, FIPS PUB 140-2, 29 (May 25, 2001), https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf [https://perma.cc/YGE6-7NVH] (Tbl. 2) (providing an overview of physical security requirements that are currently required).

[104] Exec. Order No. 14,028, Improving the Nation's Cybersecurity, 86 Fed. Reg. 26,633, § 3(a)–(d) (May 17, 2021).

systems.[105] This latter recommendation may alleviate some aforementioned concerns about malicious actors stealing private keys. Thus, in a scenario where delay-based systems are not in use, the CSA would benefit from explicitly mandating a cryptography-based, tamper-proof security system for chips.

Tamper-evident systems may also help maintain chip security, ideally making it harder for malware to compromise lower levels of the software stack.[106] Secure boots are one such system, allowing a company to monitor whether a chip is running legitimate firmware.[107] However, Tamper-control mechanisms should be used with caution. Their ability to shut down and limit parts of a chip's technical system could be exploited by adversaries to shut down legitimately located (and perhaps even U.S. located) chips.[108] Therefore, given the major national security concerns that could arise from that possibility, revisions in the CSA that explicitly address tamper-evident systems should limit the capabilities and the control they may have over a chip.

B. Enforcement Recommendations

In terms of non-technical revisions to the CSA, a centralized, government-maintained chip registry could help further prevent spoofing attempts through combining location verification with additional data contained by the registry, such as corporate ownership or operational behavior data.[109] This is addressed in a very vague fashion in the current version of the CSA, where the Secretary is given the power to "maintain a record of covered integrated circuit products that include in the record the location and current end-user of each such product".[110] However, a more explicit description of a chip registry in the CSA, including what data the chip registry could contain, may be a valuable addition to export control legislations.

---

[105] *See, e.g.*, Tom Simonite, *To Keep Passwords Safe from Hackers, Just Break Them into Bits*, MIT Tech. Rev. (Oct. 9, 2012), https://www.technologyreview.com/2012/10/09/183378/to-keep-passwords-safe-from-hackers-just-break-them-into-bits [https://perma.cc/DTU4-6XDF] (providing a relevant analogy to password protection for the potential use of threshold cryptography).

[106] Aarne et al., *supra* note 33, at 18.

[107] *Id.* at 13.

[108] Luke O'Grady, *Congress' Proposed Chip Security Act Threatens to Create New Cyber Vulnerabilities in U.S. Semiconductors*, Ctr. for Cybersecurity Pol'y & L. (July 15, 2025), https://www.centerforcybersecuritypolicy.org/insights-and-research/congress-proposed-chip-security-act-threatens-to-create-new-cyber-vulnerabilities-in-u-s-semiconductors [https://perma.cc/JAK3-AWPF].

[109] Conklin, *supra* note 64.

[110] H.R. 3447 § 4(c)(2).

Several other laws have sought to create similar requirements to this proposed chip registry in separate cybersecurity contexts. For starters, EO 14028 provides certain requirements concerning logging and retention of relevant data that arguably function in a similar manner to a chip registry.[111] In addition, the proposed (though now dead) National Cybersecurity Protection Advancement Act of 2015—in its efforts to generally enhance the sharing of information related to cybersecurity risks—suggested the developed of automated mechanisms for timely sharing of cybersecurity threat indicators.[112] That being said, the chip registry proposed here may face distinctive problems that raise similar national security concerns as with tamper-evident systems. More explicitly, centralizing information in a registry about U.S.-developed AI chips may provide an easy target for malicious actors. After gaining that information, it may then not only be easier to smuggle chips, but could also expose infrastructure-critical chips and data centers to cyberattacks. As such, there would need to be additional provisions in the CSA that ensure the security of such a registry, such as further technical measures or proposals for public-private partnerships prioritizing cybersecurity.[113]

The final recommendation for revising the CSA would be to include a provision that grants additional funding to the BIS and Department of Commerce in support of their initiatives to oversee implementation and enforcement of the CSA's requirements. As has already been mentioned, BIS has been severely underfunded despite its large workload, which has undermined its capabilities to actually enforce export controls.[114] This, coupled with inadequate due diligence, is a major contributor to the current export control issues the U.S. faces. Resolving this gap, as experts have noted, is critical for success on this front.[115] Therefore, in order to ensure that geolocation mechanisms are actually effective instead of a simple waste of resources, the CSA should grant additional funding to the organization(s)

[111] Improving the Nation's Cybersecurity, *supra* note 104, § 8(b)–(c).

[112] H.R. 1731, 114th Cong. § 3(g)(1) (2015).

[113] *See generally* Judith H. Germano, *Cybersecurity Partnerships: A New Era of Public-Private Collaboration*, The Ctr. on Law & Sec., NYU Sch. of L. 12 (2014), https://www.lawandsecurity.org/wp-content/uploads/2016/08/Cybersecurity.Partnerships-1.pdf [https://perma.cc/9TL3-UVVR] (providing examples of successes with public-private partnerships in the cybersecurity space, as a means to advocate for their increased use).

[114] Grunewald & Aird, *supra* note 19, at 16.

[115] *Id.*; *see also* Grunewald & Fist, *supra* note 80, at 28–9.

primarily responsible for monitoring and enforcing both the CSA and other relevant export control statutes.

Conclusion

This note has sought to highlight the issues with the CSA as it is currently drafted, in the hopes that lawmakers may consider revising the CSA to better address its cybersecurity vulnerabilities. The motivation for the bill itself is understandable given the current geopolitical climate, and it is not within the scope of this note to assess whether it offers the right approach from an industrial policy perspective. However, the CSA's overly ambiguous language, failure to recognize issues with current geolocation technologies, and lack of explicit enforcement measures within the text itself leaves much to be desired from a cybersecurity standpoint. Other existing statutes on similar topics do not sufficiently resolve these issues. If the CSA ever becomes enacted, it is important that these issues are addressed at both the technical and legal enforcement levels, lest it become more of an obstacle than a valuable asset. Of the many possible solutions experts could devise, this note highlights four in particular that would not only raise minimum cybersecurity standards, but also introduce additional on-chip security, centralize tracking information, and provide additional funding to relevant regulatory bodies. These proposals would likely succeed in reasonably easing cybersecurity concerns while maintaining the competitive and economic security motivations that initially inspired this bill. Therefore, if the CSA is to be a useful contribution to the export controls landscape upon enactment, it should revise its provisions to more explicitly address the cybersecurity concerns these geolocation technologies raise.