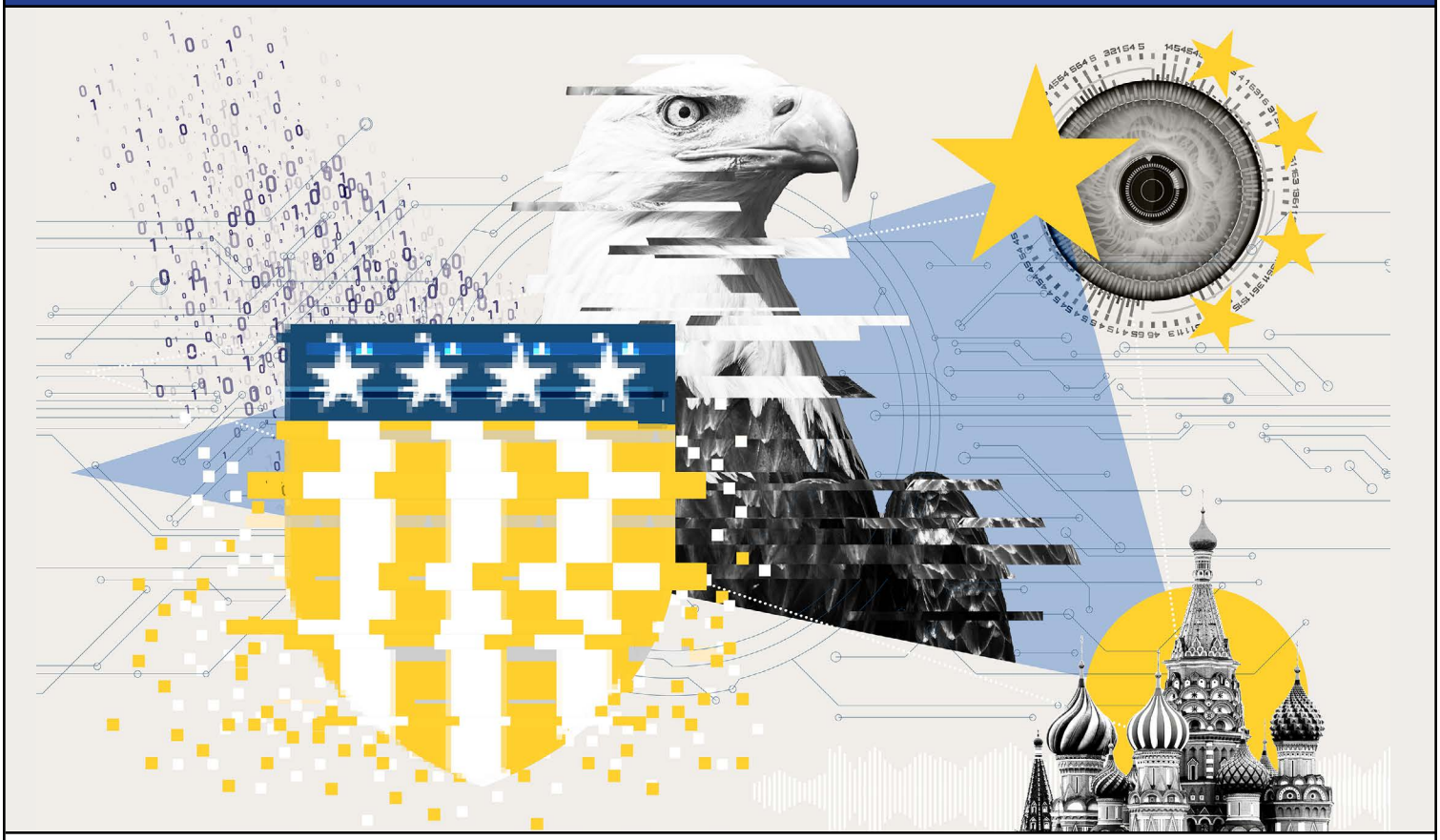
Assessing the Potential National Security Impacts of U.S. Tech Regulation

PART 1 OF 2



To foster domestic competition within the U.S. tech sector, Congress is currently considering a package of legislative proposals that would impose broad new regulatory requirements on the largest U.S. tech companies. The proposed bills encompass important issues, such as how major tech platforms handle the transfer and accessibility of users' data, application downloads, and product preferencing.

While the pending legislation is primarily concerned with addressing domestic competition in the tech sector, several provisions—as currently drafted—could bear unintended consequences for U.S. national security by exacerbating existing vulnerabilities in the domains of data privacy, cybersecurity, and the spread of mis- and disinformation. Major technology platforms face existing challenges in these spheres, but provisions in the pending legislation could carry key security implications. Select provisions in certain bills, outlined below, would introduce new legal requirements that could facilitate data collection by foreign actors, slow major U.S. tech platforms' ability to react to cyberattacks, and make combating mis- and disinformation more difficult. Underlying these issues is the rising multi-domain threat from a more assertive China, which the U.S. Department of Defense listed as the number-one priority in its 2022 National Defense Strategy.

The following analysis, produced by FP Analytics with support from the Computer Communications Industry Association (CCIA) — a trade organization that represents technologies, explores key provisions under consideration and potential impacts. While comprehensive rules and guidelines for all companies are needed to guarantee fair and safe participation in the global technology market, it is incumbent upon lawmakers to ensure that proposed legislation safeguards against extant and emerging national security risks. This analysis and the associated Virtual Dialogues are intended to advance discussion and debate on these important issues.

**The introduction of this brief was updated on June 13th, 2022, following our first virtual dialogue. Nothing in the analysis has changed since its original publication.*

This analysis was produced by FP Analytics, the independent research division of Foreign Policy, and was supported by the Computer and Communications Industry Association (CCIA). CCIA did not contribute to any of the content, nor did it have any influence over any part of this analysis. The content of this report does not represent the views of the editors of Foreign Policy magazine, ForeignPolicy.com, or any other FP publication.

FP ANALYTICS | CCIA

ISSUE 1

The U.S. lacks comprehensive data protections on par with other major economies

RELEVANT SECTIONS OF PROPOSED LEGISLATION

- *American Choice and Innovation Online Act (ACIOA) H.R. 3816, Section 2 (b) (1), Section 2 (b) (3), Section 2 (b) (4)*
- *Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act of 2021 H.R. 3849, Section 3 (a), Section 3 (b) (1), Section 4 (a), Section 4 (b) (1)*

Potential risks introduced: The American Choice and Innovation Online Act's (ACIOA) requirement that covered companies must provide data to both domestic and foreign companies upon request could compound the risk of sensitive data being compromised, including personal, corporate, and government data.

Potential national security implications: Globally, at least eighty countries,[1] including China, India, and Brazil, as well as the EU, are enacting comprehensive data privacy laws that establish widespread protections on how individuals' data can be collected, stored, and transferred. The U.S. lacks similar data protection standards, despite numerous past incidents that posed a national security risk: such as when China used stolen data to expose CIA operatives,[2] Chinese government agencies profiled prominent Western journalists and politicians,[3] and Cambridge Analytica harvested millions of users' data leading up to the 2016 election.[4] In the absence of comprehensive data privacy laws, personal, corporate, and government data collected within the U.S. remains highly accessible. This contributes to a thriving secondary market where third-party data brokers sell extensive data. For example, some of the largest U.S. data brokers provide access to data on up to 250 million U.S. consumers, composed of over 7,000 attributes on each individual available for purchase.[5] The ACIOA could worsen these risks while leaving underlying issues on how data is collected, transferred, and secured unaddressed.

Amplifying this issue is the fact that China is creating the world's most sophisticated data collection operation[6] and collects U.S. citizens' biometric data,[7] voice recordings,[8] and real-time locations.[9] Obtained through both legal[10] and illegal channels,[11] this data is being applied toward strategic aims, including identifying targets for political influence and obtaining intellectual property (IP).[12] Chinese IP theft is estimated to cost the U.S. up to $600 billion per year,[13] and protecting IP in cutting-edge technologies vital to national security, such as semiconductors and artificial intelligence (AI), calls for stronger data security measures. The regulatory regimes in the U.S. and China are such that data collected by Chinese companies in the U.S. can be moved directly to China and must be turned over to the Chinese government upon request. Widespread data collection already poses a significant threat to U.S. interests and enabling more companies, including ones with Chinese ownership, easy access to U.S. citizens, companies, and governments agencies' data could exacerbate this issue. Combating this challenge requires enacting and implementing more regulatory safeguards and protections on U.S. data prior to increasing data sharing requirements.

Major Global Data Governance Regulations

The U.S. lacks comprehensive data protections comparable to other major economies, putting U.S. data at risk.

CHINA

The Data Security Law (2021)
Expands data localization and data transfer rules and imposes penalties for violations. Places restrictions on foreign companies' ability to operate in China via increased government private-sector oversight. [14]

EUROPEAN UNION

General Data Protection Regulation (GDPR) (2018)
Establishes a comprehensive data privacy framework for EU citizens and businesses. Applies to all data intermediaries, requiring them to obtain consent before collecting or transferring data.

UNITED STATES

Clarifying Lawful Overseas Use of Data (CLOUD) (2018)
Permits law enforcement agencies to access individuals' data. There are laws that protect particular types of data, but the U.S. has no comprehensive federal law for data protection.

SOURCE: FP ANALYTICS. (2020, MAY 13). DATA GOVERNANCE POWER MAP.

ISSUE 2

Cybersecurity vulnerabilities undermine the security of critical industries, government agencies, and the nation's infrastructure

RELEVANT SECTIONS OF PROPOSED LEGISLATION

- *American Choice and Innovation Online Act (ACIOA) H.R. 3816, Section 2 (b) (5), Section 2 (c) (1)*
- *Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act of 2021 H.R. 3849, Section 4 (a), Section 4 (e) (1)*
- *Open App Markets Act S. 2710, Section 3 (d) (2), Section 3 (d) (3)*

Potential risks introduced: Conditioning security updates on Federal Trade Commission (FTC) approval and requiring major technology platforms to open up their operating systems could leave critical infrastructure vulnerable.

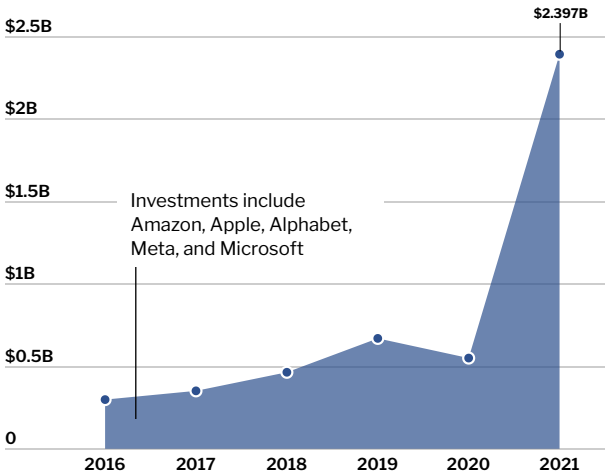
Potential national security implications: Major tech platforms store the personal data of millions of Americans[15] and are the main contractors currently providing cloud hosting infrastructure to government agencies[16],[17] and over a million private-sector companies,[18] making them integral to data and system security. The widespread integration of major tech companies' platforms into the operations of both the public and private sector make their ability to secure networks and proactively respond to cyberthreats with timely updates essential to national security. These companies have pledged a combined $30 billion investment in cybersecurity[19] over the next five years, a sixfold increase in the amount the industry contributes today[20] to strengthen defenses and prepare for evolving threats.

Proposed legislation could introduce new avenues for bad actors to access major tech platforms' operating systems. Provisions in the Open App Markets Act would limit major platforms' ability to screen apps through a centralized app store or pre-install security software. On individual devices, this could create new risks of users downloading viruses directly onto their devices. Provisions in the ACIOA and the Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act could enable widespread access to major platforms' operating systems through their requirements to make these systems widely interoperable with any company requesting access. On a technical level, the more ways a platform opens its system, the more avenues are created for potential abuse and nefarious activity.[21] Greater access could enable malicious actors to enter the software and back-end hardware systems supporting sensitive industries. [22]

If the ACCESS Act passes in its current form, the responsibility for securing data would also be distributed across the millions of applications requesting access, instead of one centralized platform.[23] Further, the ACCESS Act conditions platform patches and updates on Federal Trade Commission (FTC) review, through a newly created technical committee.[24] If a major tech platform does make an update, it would be responsible for proving that it was in the interest of user security, and competitors would be able to sue for non-compliance.[25] Conditioning updates on review by a committee that includes representatives from competitors, or potential justification through a potentially lengthy legal process, could delay a timely response to threats and impose restrictions that either prevent or actively disincentivize major tech platforms from providing robust security.

Major Platforms Cybersecurity Investments

As the rate and sophistication of cyberattacks increase, investment in cyber defense is crucial. The U.S. spends more than any other country, accounting for 76 percent of all global cybersecurity funding in 2020.[26] The largest technology platforms contribute significantly to this, investing a combined $4.7 billion on cybersecurity from 2016 through 2021.[27]



SOURCE: CB INSIGHTS

ISSUE 3

The U.S. has not established clear standards needed to effectively combat online mis- and disinformation

RELEVANT SECTIONS OF PROPOSED LEGISLATION

- *American Choice and Innovation Online Act (ACIOA) H.R. 3816, Section 2 (a) (3)*
- *Ending Platform Monopolies Act H.R. 3825, Section 2 (a) (1)*

Potential risks introduced: Proposed legislation could create new challenges in combating the spread mis- and disinformation by conceivably strengthening the position of foreign competitors and inhibiting domestic platforms' ability to invest in content moderation.

Potential national security implications: The spread of mis- and disinformation across tech platforms has posed threats to U.S. security interests abroad while inflaming domestic tensions. From Russian disinformation campaigns pushing false narratives about the 2016 election[28] and the invasion of Ukraine,[29] to widespread misinformation about the COVID-19 pandemic,[30] the spread of false narratives and propaganda has undermined fact-based discussion on key national security issues. Mis- and disinformation are prevalent across the nearly five billion[31] items shared daily by Facebook and 720,000 hours of video content uploaded daily to YouTube.[32] Major tech platforms spend hundreds of millions of dollars annually[33] on employing human content moderators and developing algorithms that can identify falsehoods and hate speech.[34] For example, Google alone has pledged $300 million over the next three years to combat online mis- and disinformation.[35] The scale of these investments highlights how severe the issues have become and illustrates the efforts necessary to rectify past missteps and existing gaps in capabilities. While major tech platforms have been used as vehicles to spread mis- and disinformation, breaking up these platforms could also limit their ability to moderate content across products and employ system-wide measures to combat mis- and disinformation.

Proposed U.S. tech regulations set no foundational rules for limiting the spread of mis- and disinformation, such as instituting identity-verification requirements for posting content on major platforms.[36] Without clear guidelines for preventing the spread of mis- and disinformation, strengthening the position of competing platforms, which lack the capital to invest in content moderation or have foreign ownership, could magnify existing challenges. Further, new limits on major tech platforms to choose which businesses they host, which are proposed in the legislation, could inhibit their ability to censor known channels of mis- and disinformation.[37] The U.S. government has an opportunity to establish and enforce broad guidelines focused on reducing the flow of mis- and disinformation within its borders. However, establishing clear standards across platforms for how content is moderated and prioritized could become increasingly difficult if content is fragmented across increasingly dispersed platforms.

LOOKING AHEAD

Ongoing debate is essential to strengthening technology regulation in the interest of national security

The digitalization of the global economy and of global data management and technology companies has brought novel and complex challenges. State and non-state actors are increasingly leveraging data and tech platforms for strategic competition. Addressing data privacy, cybersecurity, and the spread of mis- and disinformation requires comprehensive approaches applicable across the entire technology sector and close public-private collaboration. Major economies are imposing stringent rules on competition and national strategies aimed at promoting their technology sectors. In response, the U.S. will face the challenge of safeguarding national interests and investing in innovation while avoiding enacting the same protectionist policies. Clearly defined measures that address underlying and systemic issues pertaining to the entire sector will be needed to avoid inadvertently introducing new risks that undermine the U.S.'s capacity to respond and compete globally.

APPENDIX

COVERED PLATFORMS

The legislative provisions discussed in this brief would only apply to "covered platforms." There have been slight variations in definitions among laws, but the general definition as laid out in the Platform Competition and Opportunity Act of 2021 is a company that:

- Has at least 50,000,000 United States-based monthly active users on the online platform; or
- Has at least 100,000 United States-based monthly active business users on the platform;
- Is owned or controlled by a person, with net annual sales, or a market capitalization greater than $600,000,000,000, adjusted for inflation on the basis of the Consumer Price Index, at the time of the Commission's or the Department of Justice's designation under section 4(a) or any of the two years preceding that time, or at any time in the 2 years preceding the filing of a complaint for an alleged violation of this Act; and
- Is a critical trading partner for the sale or provision of any product or service offered on or directly related to the online platform.

PROVISIONS REFERENCED

American Choice and Innovation Online Act (ACIOA) H.R. 3816

- Section 2 (a) (3)

  (a) Violation.—It shall be unlawful for a person operating a covered platform, in or affecting commerce, to engage in any conduct in connection with the operation of the covered platform that… (3) discriminates among similarly situated business users.

- Section 2 (b) (1), (3), (4), (5)

  (b) Other Discriminatory Conduct.—It shall be unlawful for a person operating a covered platform, in or affecting commerce, to—(1) restrict or impede the capacity of a business user to access or interoperate with the same platform, operating system, hardware and software features that are available to the covered platform operator's own products, services, or lines of business; (3) use non-public data obtained from or generated on the platform by the activities of a business user or its customers that is generated through an interaction with the business user's products or services to offer or support the offering of the covered platform operator's own products or services; (4) restrict or impede a business user from accessing data generated on the platform by the activities of the business user or its customers through an interaction with the business user's products or services, such as contractual or technical restrictions that prevent the portability of such data by the business user to other systems or applications; (5) restrict or impede covered platform users from un-installing software applications that have been preinstalled on the covered platform or changing default settings that direct or steer covered platform users to products or services offered by the covered platform operator;

- Section 2 (c) (1)

  (c) Affirmative Defense.—(1) IN GENERAL.—Subsection (a) and (b) shall not apply if the defendant establishes by clear and convincing evidence that the conduct described in subsections (a) or (b)— (A) would not result in harm to the competitive process by restricting or impeding legitimate activity by business users; or (B) was narrowly tailored, could not be achieved through a less discriminatory means, was nonpretextual, and was necessary to—(i) prevent a violation of, or comply with, Federal or State law; or (ii) protect user privacy or other non-public data.

Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act of 2021 H.R. 3849

- Section 3 (a)

  (a) In General.—A covered platform shall maintain a set of transparent, third-party-accessible interfaces (including application programming interfaces) to enable the secure transfer of data to a user, or with the affirmative consent of a user, to a business user at the direction of a user, in a structured, commonly used, and machine-readable format that complies with the standards issued pursuant to section 6(c).

- Section 3 (b) (1)

  (b) Data Security.—(1) IN GENERAL.—A competing business or a potential competing business that receives ported user data from a covered platform shall reasonably secure any user data it acquires, and shall take reasonable steps to avoid introducing security risks to data or the covered platform's information systems.

- Section 4 (a)

  (a) In General.—A covered platform shall maintain a set of transparent, third-party-accessible interfaces (including application programming interfaces) to facilitate and maintain interoperability with a competing business or a potential competing business that complies with the standards issued pursuant to section 6(c).

- Section 4 (b) (1)

  (b) Data Security.—(1) IN GENERAL.—A competing business or a potential competing business that accesses an interoperability interface of a covered platform shall reasonably secure any user data it acquires, processes, or transmits, and shall take reasonable steps to avoid introducing security risks to user data or the covered platform's information systems.

- Section 4 (e) (1)

  (e) Prohibited Changes To Interfaces.—(1) COMMISSION APPROVAL.—A covered platform may make a change that may affect its interoperability interface by petitioning the Commission to approve a proposed change. The Commission shall allow the change if, after consulting with the relevant technical committee the Commission concludes that the change is not being made with the purpose or effect of unreasonably denying access or undermining interoperability for competing businesses or potential competing businesses.

Open App Markets Act S. 2710

- Section 3 (d) (2), (3)

  Interoperability.—A covered company that controls the operating system or operating system configuration on which its app store operates shall allow and provide readily accessible means for users of that operating system to—(2) install third-party apps or app stores through means other than its app store; and (3) hide or delete apps or app stores provided or preinstalled by the app store owner or any of its business partners.

Ending Platform Monopolies Act H.R. 3825

- Section 2(a) (1)

  (a) Violation.—As of the date an online platform is designated as a covered platform under subsection 6(a), it shall be unlawful for a covered platform operator to own, control, or have a beneficial interest in a line of business other than the covered platform that—(1) utilizes the covered platform for the sale or provision of products or services.

ENDNOTES

1 FP Analytics. (2020, October 6). Global Data Governance. Foreign Policy Magazine. https://foreignpolicy.com/2020/10/06/global-data-privacy-collection-laws-database-surveillance-cybersecurity-governance/

2 Dorfman, Z. (2020, December 21). China Used Stolen Data to Expose CIA Operatives in Africa and Europe. Foreign Policy. https://foreignpolicy.com/2020/12/21/china-stolen-us-data-exposed-cia-operatives-spy-networks/

3 Cadell, C. (2021, December 31). China harvests masses of data on Western targets, documents show. The Washington Post. https://www.washingtonpost.com/national-security/china-harvests-masses-of-data-on-western-targets-documents-show/2021/12/31/3981ce9c-538e-11ec-8927-c396fa861a71_story.html

4 Lapowsky, I. (2019, March 17). How Cambridge Analytica Sparked the Great Privacy Awakening. Wired. https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/

5 Sherman, J. (2021). Report: Data Brokers and Sensitive Data on U.S. Individuals. Duke University. https://sites.sanford.duke.edu/techpolicy/report-data-brokers-and-sensitive-data-on-u-s-individuals/

6 Balding, C. (2021, November 29). China's Collection of Data on Foreigners Is a National Security Risk. Discourse Magazine. https://www.discoursemagazine.com/politics/2021/11/29/chinas-collection-of-data-on-foreigners-is-a-national-security-risk/#:~:text=The%20BGI%20Group%2C%20a%20Chinese,on%20Americans%20and%20other%20foreigners

7 Wertheim, J. (2021, January 31). China's push to control Americans' health care future. CBS News. https://www.cbsnews.com/news/biodata-dna-china-collection-60-minutes-2021-01-31/

8 Hoffman, S. (2021, January 7). The U.S.-China Data Fight Is Only Getting Started. Foreign Policy Magazine. https://foreignpolicy.com/2021/07/22/data-tiktok-china-us-privacy-policies/

9 Collier, K. (2020, February 10). China spent years collecting Americans' personal information. The U.S. just called it out. NBC News. https://www.nbcnews.com/tech/security/china-spent-years-collecting-americans-personal-information-u-s-just-n1134411

10 Choi, J. (2021, December 31). Documents show Chinese government collects droves of data from Western social media: report. The Hill. https://thehill.com/policy/international/china/587839-documents-show-chinese-government-collects-droves-of-data-from/

11 Nakashima, E. (2015, June 5). With a series of major hacks, China builds a database on Americans. The Washington Post. https://www.washingtonpost.com/world/national-security/in-a-series-of-hacks-china-appears-to-building-a-database-on-americans/2015/06/05/d2af51fa-0ba3-11e5-95fd-d580f1c5d44e_story.html

12 Balding, C. (2020, November 3). Chinese Open-Source Data Collection, Big Data, And Private Enterprise Work for State Intelligence and Security: The Case of Shenzhen Zhenhua. SSRN. https://dx.doi.org/10.2139/ssrn.3691999

13 America is struggling to counter China's intellectual property theft. (2022, April 18). The Financial Times. https://www.ft.com/content/1d13ab71-bffd-4d63-a0bf-9e9bdfc33c39

14 Perez, C. (2022, January 28). Why China's New Data Security Law Is a Warning for the Future of Data Governance. Foreign Policy Magazine. https://foreignpolicy.com/2022/01/28/china-data-governance-security-law-privacy/

15 Novet, J. (2018, February 11). The case for Apple to sell a version of iCloud for work. CNBC. https://www.cnbc.com/2018/02/11/apple-could-sell-icloud-for-the-enterprise-barclays-says.html

16 Microsoft. (n.d.). Azure for US Department of Defense. https://azure.microsoft.com/en-us/global-infrastructure/government/dod/

17 Burton, T. (2021, October 7). AWS wins coveted approval to host federal government data. Financial Review. https://www.afr.com/technology/aws-wins-coveted-approval-to-host-federal-government-data-20211007-p58y22

18 Gillard, M. (2020, January 28). Who's Using Amazon Web Services? [2020 Update]. Contino. https://www.contino.io/insights/whos-using-aws

19 Hardcastle, J. (2021, August 25). Tech Giants Commit $30B to Cybersecurity After White House Meeting. SDX Central. https://www.sdxcentral.com/articles/news/tech-giants-commit-30b-to-cybersecurity-after-white-house-meeting/2021/08/

20 CB Insights. (2022, January 11). The Big Tech in Cybersecurity Report: How Facebook, Apple, Microsoft, Google, & Amazon Are Tackling Cyber Threats. https://www.cbinsights.com/research/report/famga-big-tech-cybersecurity/

21 Lewis, J. (2020, January 27). Cybersecurity and the Problem of Interoperability. Center for Strategic and International Studies. https://www.csis.org/analysis/cybersecurity-and-problem-interoperability

22 Goure, D. (2022, February 7). Senate Attack on Big Tech Will Harm U.S. Economic and National Security. The National interest. https://nationalinterest.org/feature/senate-attack-big-tech-will-harm-us-economic-and-national-security-200423

23 Bolton, T. (2021, November 13). Security in Antitrust: Implications of Two House Bills. R Street. https://www.rstreet.org/2021/11/13/security-in-antitrust-implications-of-two-house-bills/

24 The Flawed ACCESS Act Creates More Problems Than It Solves. (2021, June 22). National Taxpayers Union Foundation. https://www.ntu.org/foundation/detail/the-flawed-access-act-creates-more-problems-than-it-solves

25 Riley, T. (2022, January 24). Security fears over antitrust legislation raise looming questions about a federal privacy law. CyberScoop. https://www.cyberscoop.com/security-fears-over-antitrust-legislation-raise-looming-questions-about-a-federal-privacy-law/

26 Crunchbase. (2021). Report: The Rise of Global Cybersecurity Venture Funding. https://about.crunchbase.com/cybersecurity-research-report-2021/

27 CB Insights. (2022, March 9). Big Tech's Playbook: Where Facebook, Amazon, Microsoft, Google, and Apple are investing & acquiring — and what it signals about the future. https://www.cbinsights.com/research/report/big-tech-investments-acquisitions/

28 Niu, I., Bracken, K., and Eaton, A. (2020, October 25). Russia Created an Election Disinformation Playbook. Here's How Americans Evolved It. The New York Times. https://www.nytimes.com/2020/10/25/video/russia-us-election-disinformation.html

29 Brown, S. (2022, April 6). In Russia-Ukraine war, social media stokes ingenuity, disinformation. Massachusetts Institute of Technology. https://mitsloan.mit.edu/ideas-made-to-matter/russia-ukraine-war-social-media-stokes-ingenuity-disinformation

30 Otto, L. (2021, December 30). Mapping the harm of COVID-19 misinformation on social media. University of Wisconsin Milwaukee. https://uwm.edu/news/mapping-the-harm-of-covid-19-misinformation-on-social-media/

31 41 Up-to-Date Facebook Facts and Stats. (n.d.). Wishpod. https://blog.wishpond.com/post/115675435109/40-up-to-date-facebook-facts-and-stats#:~:text=24%20.,by%20Facebook%20users%20each%20day.

32 Wise, J. (2022, May 8). How Many Videos Are Uploaded to YouTube a Day in 2022? EarthWeb. https://earthweb.com/how-many-videos-are-uploaded-to-youtube-a-day/#:~:text=11.1)%20Related%20Reading-,How%20Many%20Videos%20are%20Uploaded%20to%20YouTube%20a%20Day%202022,new%20video%20uploads%20per%20hour

33 Satariano, A. and Isaac, M. (2021, August 31). The Silent Partner Cleaning Up Facebook for $500 Million a Year. The New York Times. https://www.nytimes.com/2021/08/31/technology/facebook-accenture-content-moderation.html?smid=url-share

34 Tham, I. (2021, June 1). AI to power Google's battle against fake news. The Straits Times. https://www.straitstimes.com/tech/tech-news/ai-to-power-googles-battle-against-fake-news-0

35 Roose, K. (2018, March 20). Google Pledges $300 Million to Clean Up False News. The New York Times. https://www.nytimes.com/2018/03/20/business/media/google-false-news.html

36 Identity verification is critical to combating misinformation and extremist content online. (n.d.). Onfido. https://onfido.com/resources/blog/identity-verification-is-critical-to-combating-misinformation-and-extremist-content-online

37 Karr, T. (2022, January 20). Provisions in Senate Antitrust Bill Would Undermine the Fight Against Online Hate and Disinformation. Free Press. https://www.freepress.net/news/press-releases/provision-senate-antitrust-bill-would-undermine-fight-against-online-hate-and-disinformation

Graphics Sources:

Major Global Data Governance Regulations -

FP Analytics. (2021, September 15). Global Data Governance. Foreign Policy Magazine. https://foreignpolicy.com/2020/10/06/global-data-privacy-collection-laws-database-surveillance-cybersecurity-governance/

Perez, C. (2022, January 28). Why China's New Data Security Law Is a Warning for the Future of Data Governance. Foreign Policy Magazine. https://foreignpolicy.com/2022/01/28/china-data-governance-security-law-privacy/

Major Platforms Cybersecurity Investments -

CB Insights. (2022, March 9). Big Tech's Playbook: Where Facebook, Amazon, Microsoft, Google, and Apple are investing & acquiring — and what it signals about the future. https://www.cbinsights.com/research/report/big-tech-investmentsacquisitions/