



TEARING DOWN WALLED GARDENS: ENCOURAGING ADVERSARIAL INTEROPERABILITY TO PROMOTE COMPETITION



BY
LUKE HOGG

Luke Hogg is policy manager at Lincoln Network, where he focuses on the intersection of emerging technologies and public policy.

THE INTEROPERABILITY HOPE

By Joshua Gans



MANDATED INTEROPERABILITY: THE CURE IS WORSE THAN THE DISEASE

By Jay Ezrielev



REDUCING BARRIERS TO ENTRY AND HEDGING AGAINST OBSOLESCENCE WITH SMART GRID INTEROPERABILITY

By Cheyney O'Fallon & Avi Gopstein



TEARING DOWN WALLED GARDENS: ENCOURAGING ADVERSARIAL INTEROPERABILITY TO PROMOTE COMPETITION

By Luke Hogg



INTEROPERABILITY AS A REMEDY IN ANTITRUST CASES

By Mitch Stoltz



THE PROPOSED U.S. ACCESS ACT MANDATING INTEROPERABILITY WILL NOT UNLEASH COMPETITION IN SOCIAL NETWORKING: HERE'S HOW TO FIX IT

By Cristian Santesteban



TEARING DOWN WALLED GARDENS: ENCOURAGING ADVERSARIAL INTEROPERABILITY TO PROMOTE COMPETITION

By Luke Hogg

The concentration of the Internet economy behind the walled gardens of a select few companies has led policymakers across the political spectrum to call for congressional action. However, most legislation proposed thus far takes an overly punitive approach to Big Tech that is unlikely to create the conditions necessary for a truly competitive digital environment. A better way to promote competition in digital markets is by encouraging upstart companies to adversarially interoperate with dominant platforms. Large online platforms have weaponized the Computer Fraud and Abuse Act and other laws to ward off nascent competitors, making adversarial interoperability difficult. To open up the digital economy, lawmakers should turn their attention to reforming portions of the CFAA to prevent its abuse. By doing so, Congress would take a significant step toward reopening the Internet.

Visit www.competitionpolicyinternational.com for access to these articles and more!

Scan to Stay Connected!

Scan here to subscribe to CPI's **FREE** daily newsletter.



01

INTRODUCTION

As it emerged from its embryonic phase of government-supported experimentation, the Internet was open and protocol-driven. Looking at new commercial frontiers, upstart companies built radical new technologies and iterated on each other's successes. This adversarial environment was hyper-competitive in a way that few markets have ever been, and it matured through boom-and-bust cycles. But today, the concentration of the Internet's tech stack among a few large companies has created a closed ecosystem of walled gardens and points of control, causing many policymakers to ask how the government can begin bringing competition back to digital markets. Following a wave of increased scrutiny, antitrust enforcement agencies have filed numerous lawsuits against large online platforms, and lawmakers are considering legislation intended to strictly regulate or break up Big Tech firms.

Most of the attention on addressing online market concentration has focused on imposing new restrictions on Big Tech. However, such a punitive approach will not necessarily result in the expansion of competition for which proponents wish. Rather than restricting incumbents, policymakers should seek ways of allowing startups to challenge dominant firms, such as the promotion of adversarial interoperability: the process of interoperating with a product or service without permission. Any successful attempt to promote adversarial interoperability will need to address one of the primary tools that technology companies have used to destroy competitors: the Computer Fraud and Abuse Act ("CFAA").

This law was originally intended to prevent hacking by making unauthorized computer access a federal crime, but companies have consistently abused the civil component of the CFAA to sue competitors out of existence for adversarially interoperating. Now that policymakers are seeking ways to rein in Big Tech, it is time to reform the civil provision of the CFAA and encourage more adversarial interoperability.

02

BIG TECH AND ANTITRUST IN THE SPOTLIGHT

In recent years, the rapid decline of public trust in large technology companies has spurred a radical shift in how regulators and policymakers approach Big Tech.² Once the exemplars of American ingenuity and innovation, some of Silicon Valley's biggest success stories are now seen as "enemies of the people."³ While Democrats and Republicans disagree about many perceived issues with Big Tech, many lawmakers on both sides of the aisle agree that market dominance of a select few online platforms is problematic.

The mammoth 2021 House Judiciary Committee report on competition in digital markets typifies Democrats' approach to Big Tech.⁴ Chairman Jerry Nadler's (D-NY) introduction states in no uncertain terms that Amazon, Apple, Facebook, and Google each serve as gatekeepers over portions of our digital economy and "each platform uses its gatekeeper position to maintain its market power."⁵ Many Republicans share this perspective. As Sen. Chuck Grassley (R-IA), Ranking Member of the Senate Judiciary Committee, stated at the introduction of the American Innovation and Choice Online Act:

As Big Tech has grown and evolved over the years, our laws have not changed to keep up and ensure these companies are competing fairly. These companies have continued to become a larger part of our everyday lives and the global economy, controlling what we see and how we engage on the internet. Big Tech needs to be held accountable if they behave in a discriminatory manner.⁶

Bipartisan coalitions in the Senate have introduced legislation that would impose new restrictions on the business practices of online platforms. For example, the American Innovation and Choice Online Act ("AICOA") sponsored by Sen. Amy Klobuchar (D-MN) and co-sponsored by Sen. Chuck Grassley (R-IA) would prohibit large online platforms from preferencing their own products and services over

2 Ina Fried, *Americans' trust in tech companies hits new low*, Axios (April 7, 2022), <https://www.axios.com/2022/04/07/trust-tech-companies-new-low-americans>.

3 *Big Tech Companies Are 'Enemies of the People': Heritage President Kevin Roberts on Newsmax, WMAL*, Heritage Foundation (Feb. 14, 2022), <https://www.heritage.org/press/big-tech-companies-are-enemies-the-people-heritage-president-kevin-roberts-newsmax-wmal>.

4 Staff of H. Comm. on the Judiciary, 116th Cong, *Investigation of Competition in Digital Markets*, (Comm. Print, 2020).

5 *Id.* at 6.

6 Press Release, Sen. Amy Klobuchar, Klobuchar, Grassley, Colleagues to Introduce Bipartisan Legislation to Rein in Big Tech (October 14, 2021), <https://www.klobuchar.senate.gov/public/index.cfm/2021/10/klobuchar-grassley-colleagues-to-introduce-bipartisan-legislation-to-rein-in-big-tech>.

those of third parties.⁷ The Open App Markets Act, sponsored by Sens. Klobuchar and Marsha Blackburn (R-TN), would require tech companies to allow third-party applications and app stores to be side-loaded and would prohibit these companies from controlling in-app payment systems as a condition of distribution.⁸ The Tougher Enforcement Against Monopolists (“TEAM”) Act from Sen. Mike Lee (R-UT) would codify the consumer welfare standard and create a statutory presumption against mergers that would result in market share of over 33 percent.⁹

Concerns about the growing market dominance of Big Tech are not confined to Congress alone. President Biden’s Executive Order on Promoting Competition in the American Economy affirmed that it is the policy of his administration to “combat the excessive concentration of industry, the abuses of market power, and the harmful effects of monopoly and monopsony,” especially among online platforms.¹⁰ The elevation of Lina Khan — a woman who rose to fame on the back of a *Yale Law Review* article criticizing the anticompetitive dominance of Amazon — to head the Federal Trade Commission (“FTC”) is further evidence that the tide has shifted against Big Tech.¹¹

Federal regulators have already begun focusing their attention on Big Tech. The FTC filed a lawsuit against Facebook (now Meta) alleging that the company has monopolized the market for social media through an “illegal buy-or-bury scheme.”¹² The Department of Justice is litigating an antitrust suit against Google that alleges the company used anticompetitive practices to maintain a monopoly in the online search and advertising markets.¹³ Apple¹⁴ and Amazon¹⁵ are both reportedly being investigated for antitrust violations and facing potential federal enforcement actions.

“Concerns about the growing market dominance of Big Tech are not confined to Congress alone”

Congressional intent with all these proposals is twofold: punish and restrict “Big Tech,” and allow for more innovation and entrants into digital markets. But creating the conditions under which new market entrants can thrive and compete against entrenched incumbents is far more difficult than levying massive fines or increasing the costs of regulatory compliance.¹⁶ The current approach is analogous to playing whack-a-mole; once a certain business practice is banned, large companies have the resources to pivot and find novel ways of maintaining dominance, while new entrants are left determining how to comply.

The fundamental issue that few lawmakers seem willing to grapple with is that the United States’ policies allowed, if not created, a closed Internet ecosystem. When the Internet was in its infancy, it was a deeply decentralized place built on open protocols. Over time, entrepreneurs were able to centralize various aspects of the digital economy, earning fortunes that enabled them to further consolidate.¹⁷ These companies used their newfound power to create an array of walled gardens: the move toward centralized platforms and cloud hosting has given a few large players enormous control over what happens in online markets.

7 American Innovation and Choice Online Act, S. 2992, 117th Cong. § 2 (2021).

8 Open App Markets Act, S. 2710, 117th Cong. § 2 (2021).

9 Tougher Enforcement Against Monopolists (TEAM) Act, S. 2039, 117th Cong. § 1 (2021).

10 Exec. Order No. 14,036, 86 Fed. Reg. 36,987 (July 14, 2021).

11 Lina M. Khan, *Amazon’s Antitrust Paradox*, 126 Yale L.J. 3, 710-805 (2017).

12 Press Release, Federal Trade Commission, FTC Alleges Facebook Resorted to Illegal Buy-or-Bury Scheme to Crush Competition After String of Failed Attempts to Innovate (August 19, 2021), <https://www.ftc.gov/news-events/news/press-releases/2021/08/ftc-alleges-facebook-resorted-illegal-buy-or-bury-scheme-crush-competition-after-string-failed>.

13 Press Release, Department of Justice Office of Public Affairs, Justice Department Sues Monopolist Google For Violating Antitrust Laws (October 20, 2020), <https://www.justice.gov/opa/pr/justice-department-sues-monopolist-google-violating-antitrust-laws>.

14 Josh Sisco, *Apple faces growing likelihood of DOJ antitrust suit*, Politico (August 26, 2022), <https://www.politico.com/news/2022/08/26/justice-department-antitrust-apple-00053939>.

15 Leah Nysten, *FTC’s Antitrust Probe of Amazon Picks Up Speed Under New Boss*, Bloomberg (May 31, 2022), <https://www.bloomberg.com/news/articles/2022-05-31/ftc-s-antitrust-probe-of-amazon-picks-up-speed-under-new-boss>.

16 Carl Benedikt Frey and Giorgio Presidente, *The GDPR effect: How data privacy regulation shaped firm performance globally*, Centre for Economic Policy Research (March 10, 2022), <https://cepr.org/voxeu/columns/gdpr-effect-how-data-privacy-regulation-shaped-firm-performance-globally>.

17 See generally, *Consolidation in the Internet Economy*, Internet Society (2019), <https://future.internetsociety.org/2019/wp-content/uploads/sites/2/2019/04/InternetSociety-GlobalInternetReport-ConsolidationintheInternetEconomy.pdf>.

Policymakers are right to be skeptical of the control exerted by large online platforms. But the punitive approach to Big Tech could harm both consumers and markets by overly restricting products and services that consumers enjoy. Rather than running this risk, policymakers should seek ways of encouraging competitors to build off the success of major incumbents. The best way to do this is by deregulating to remove barriers to adversarial interoperability.

03

ADVERSARIAL INTEROPERABILITY

Interoperability is the ability for different products or services to work with each other. Sometimes interoperability is indifferent or even intentional, as was the case with the advent of the standards for Bluetooth technologies: any two devices that are Bluetooth enabled can interact with each other. But such intentional and harmonious interoperability is the exception, rather than the rule. More often than not, major competitive innovations have come from adversarial relationships in which developers create products and services that work with existing systems against the wishes of the incumbent company.

The early days of the Internet were marked by competitive adversarial interoperability:

Scratch the surface of most Big Tech giants and you'll find an adversarial interoperability story: Facebook grew by making a tool that let its users stay in touch with MySpace users; Google products from search to Docs and beyond depend on adversarial interoperability layers; Amazon's cloud is full of virtual machines pretending to be discrete CPUs, impersonating real computers so well that the programs running within them have no idea that they're trapped in the Matrix. Adversarial interoperability converts market dominance from an unassailable asset to a liability.¹⁸

Adversarial interoperability is an essential component of a competitive Internet ecosystem. It lowers barriers to entry

for new firms by allowing them to access the network effects of incumbent players.

Consider author Cory Doctorow's example of Facebook.¹⁹ Facebook's early success was due in no small part to its ability to build on the success of MySpace. Allowing its own users to link their Facebook and MySpace accounts, and even send messages from Facebook to MySpace, made it simple for users to switch back and forth. Facebook did this in spite of MySpace's safeguards. Now that Facebook has achieved success on the back of MySpace, it and other Big Tech firms have been able to use the law to prevent other firms from taking advantage of the very kind of adversarial interoperability that made them successful.

At least one court has recognized the power of adversarial interoperability to increase competition. In the early 1990s, the company Accolade bought and disassembled a Sega Genesis video game console for the purpose of creating compatible games. Sega sued Accolade under copyright law, but the Ninth Circuit Court of Appeals ruled in favor of Accolade. In its opinion, the court held that Accolade's work "led to an increase in the number of independently designed video game programs offered for use with the Genesis console."²⁰

Thought leaders in technology policy, such as Stanford professor Francis Fukuyama, also recognize the importance of adversarial interoperability in maintaining healthy digital markets. What Fukuyama dubs middleware — "software, provided by a third party and integrated into the dominant platforms, that would curate and order the content that users see" — could reinvigorate competition in a stagnating social media ecosystem:

Middleware facilitates competition. It offers a new and distinct layer of potential competition for consumer loyalties and opens a pathway for innovations in managing information, including commercial information that might benefit firms otherwise disadvantaged by the platforms' business models. It could also open lucrative markets both for technology companies that can improve platform functionality and for civic organizations that want to participate in political and social discourse.²¹

Social media sites are not the only digital market where adversarial interoperability can increase competition. The U.K.'s Digital Competition Expert Panel, for example, re-

18 Cory Doctorow, *Adversarial Interoperability: Reviving an Elegant Weapon From a More Civilized Age to Slay Today's Monopolies*, Electronic Frontier Foundation (June 7, 2019), <https://www.eff.org/deeplinks/2019/06/adversarial-interoperability-reviving-elegant-weapon-more-civilized-age-slay> (Doctorow is an author and special advisor to the Electronic Frontier Foundation).

19 *Id.*

20 *Sega Enterprises Ltd. v. Accolade, Inc.*, 977 F.2d 1510 (9th Cir. 1992).

21 Francis Fukuyama, Barak Richman, Ashish Goel, Robert R. Katz, A. Douglas Melamed, Marietje Schaak, *Middleware for Dominant Digital Platforms: A Technological Solution for a Threat to Democracy* (Stanford University Cyber Policy Center), 3, 6, https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/cpc-middleware_ff_v2.pdf.

leased a prominent report in 2018 finding that digital markets are especially susceptible to tipping, “in which a winner will take most of the market” and then vehemently protect that market.²² The report also noted that government policy and regulations have a limited ability to increase competition in digital markets. To address these challenges, the report, in one of its primary recommendations, urged the government to “use data openness as a tool to promote competition.”²³

It is only natural for companies to attempt to impede adversarially interoperable competition. Most large tech companies devote significant resources into protecting their platforms through technical means. However, incumbent firms have taken advantage of laws, most of all the CFAA, to prevent adversarial interoperability.

04 THE COMPUTER FRAUD AND ABUSE ACT

Signed into law by President Reagan in 1986, the CFAA was one of the federal government’s first legislative attempts to address the threat of computer hacking. The law is divided into two parts: criminal and civil. The criminal component allows the Department of Justice to prosecute individuals for intentionally accessing a computer without authorization with the intent to defraud, extort, obtain information, or transmit information.²⁴ It also allows individuals or companies damaged by an activity covered by the CFAA to obtain compensatory damages and, perhaps more importantly, injunctive relief against the violator in federal civil court.²⁵

The law had an unlikely inspiration: the 1983 film *WarGames*, in which a high school student played by Mathew Broderick inadvertently hacks into a military supercomputer, nearly

causing a thermonuclear war with the Soviet Union.²⁶ According to author Fred Kaplan, the movie greatly concerned President Reagan. After hearing from then-Chairman of the Joint Chiefs of Staff Gen. John W. Vessey, Jr. that “the problem is much worse than you think,” the president turned to Congress for immediate legislative action.²⁷ The movie even came up in congressional discussions about the bill that would become the CFAA.²⁸

While the criminal component of the CFAA has been the subject of public policy debates since its passage, it is not the most important passage for companies seeking to overwhelm their competition. More significant from the standpoint of hampering adversarial interoperability is the civil provision. One company that has used this provision to devastating effect is the same company currently tussling with federal antitrust enforcers over anticompetitive practices: Facebook.

05 A CASE STUDY IN CFAA ABUSE: FACEBOOK vs. POWER.COM

In December of 2008, Facebook — then a fledgling social media company — filed a rather unique lawsuit that would become crucial to the struggle between two competing visions of the Internet.²⁹ A tech startup, Power.com, built an online platform that allowed users to aggregate disparate social media accounts in one place. Essentially, Power had adversarially built a system that allowed users to interoperate with Facebook and other social media sites independently from their native ecosystems by scraping and proxying those websites. Users could see their contacts and post

22 Digital Competition Expert Panel, *Unlocking digital competition: Report of the Digital Competition Expert Panel*, 4-6 (March 2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf.

23 *Id.* at 9.

24 Computer Fraud and Abuse Act, Pub. L. No. 99-474, 100 Stat. 1213 (1986) (codified as amended at 18 U.S. Code § 1030).

25 *Id.*

26 Fred Kaplan, ‘*WarGames*’ and Cybersecurity’s Debt to a Hollywood Hack, *N.Y. Times* (February 19, 2016), <https://www.nytimes.com/2016/02/21/movies/wargames-and-cybersecuritys-debt-to-a-hollywood-hack.html>.

27 *Id.*

28 H.R. Rep. No. 98-894, at 10 (1984).

29 Complaint, *Facebook, Inc. v. Power Ventures, Inc.*, No. 08-5780, (N.D. Cal. Oct. 22, 2009) *aff’d* in part 844 F.3d 1058 (9th Cir. 2016).

to their different social media accounts all from Power's dashboard.

Power received little publicity until it began a promotional campaign in 2008. To attract customers, Power incentivized its users to send messages to their friends through Facebook encouraging them to join Power. When Facebook learned of the campaign, it initiated an internet protocol ("IP") block and sent Power a cease and desist letter. Power persisted, changing its IP address and ignoring the cease and desist. Facebook then sued Power for violating the CFAA, among other claims.

After years of litigation against the defunct social media company and its founder, the Ninth Circuit Court of Appeals upheld a lower court ruling in Facebook's favor in 2016.³⁰ Most notably, the court held that Power had gained unauthorized access to Facebook's system after receiving the cease and desist and thus was civilly liable under the CFAA.

The Ninth Circuit's opinion asserted that "initially, Power users arguably gave Power permission to use Facebook's computers to disseminate messages."³¹ By signing up for Power's service, users gave authorization for Power to access Facebook's servers on the user's behalf. But, in the Court's view, Facebook's cease and desist letter "expressly rescinded that permission," turning authorized access into unauthorized access.³² The fact that Facebook took active measures to prevent Power from accessing its servers through an IP block bolstered this interpretation. The Ninth Circuit further explained: "The consent that Power had received from Facebook users was not sufficient to grant continuing authorization to access Facebook's computers after Facebook's express revocation of permission."³³ The implication was that under the CFAA, a user's data is not theirs to do with as they wish. It is, at least in part, owned and controlled by Facebook.

After nine years of litigation in federal court, Facebook was awarded a mere \$79,640.50 in compensatory damages.³⁴ But money was never the point. Facebook also received a permanent injunction against Power. Facebook's case against Power was not about material harm to Facebook; it was about using the law and courts to kill a potential competitor. In that effort, Facebook clearly succeeded. *Facebook v. Power.com* demonstrates that the CFAA — a law

intended to prevent cybercrime — can be used to squash competition.

06

REFORMING THE CFAA TO ENCOURAGE ADVERSARIAL INTEROPERABILITY

As discussed above, lawmakers concerned with the market dominance of large online platforms have focused their attention on debating legislation to break up Big Tech. Few, if any, have considered how existing laws enable these companies to secure their walled gardens. One of the best ways policymakers can encourage competition in digital markets is by eliminating some of the tools that have been used to thwart competition. Two policy proposals that have been put forward in recent years deserve attention for their attempt to encourage a more open Internet ecosystem and more adversarial interoperability by addressing flaws in existing law.

In 2015, Sen. Ron Wyden (D-OR) and Rep. Zoe Lofgren (D-CA) introduced companion legislation known as Aaron's Law that intended to clarify the meaning of unauthorized access in the CFAA.³⁵ Aaron's Law would have replaced the term "exceeds authorized access" with "access without authorization," defining the new term as obtaining information on a protected computer that the accessor lacks authorization to and knowingly circumventing measures designed to prevent unauthorized access. It also would have removed some redundancies from the CFAA and limited some penalties for violation.

While Aaron's Law may have clarified what constitutes unauthorized access, it would have done little to open up digital markets to adversarial interoperability. Tech companies implement firewalls and other systems to prevent unauthorized access. Truly competitive adversarial interoperability of the type Power was engaged in requires going a step further and finding ways around measures intended to keep competitors out. Such activity likely would still be banned under Aaron's Law. In any case, the Supreme Court re-

30 *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058 (9th Cir. 2016).

31 *Id.* at 1067.

32 *Id.* at 1067.

33 *Id.* at 1068.

34 *Facebook, Inc. v. Power Ventures, Inc., et al.*, 252 F.Supp.3d 765 (2017).

35 Aaron's Law Act of 2015, S. 1030 and H.R. 1918, 114th Cong. § 1 (2015).

cently narrowed the interpretation of what activity “exceeds authorized access” to exclude many of the activities that would have been allowed under Aaron’s Law, rendering the proposal mostly moot.³⁶

A more recent proposal from Sen. Mark Warner (D-VA) and Rep. Mary Scanlon (D-PA-5) takes a more burdensome approach to promoting interoperability. The Augmenting Compatibility and Competition by Enabling Service Switching (“ACCESS”) Act would mandate data portability and interoperability.³⁷ It would direct all large communications platforms to maintain accessible application programming interfaces that allow interoperable communication with other large platforms and allow users to transfer their data to competing platforms.

One strength of the ACCESS Act is its delegatability provision, which directs large platforms to maintain open interfaces that allow users to delegate management of their interactions, content, and account settings to a third party. Such a provision would help realize the future envisioned by Fukuyama, in which content is managed by a suite of third-party applications built on top of existing platforms. However, the ACCESS Act also contains restrictions stipulating that no third party can use the mandated programming interfaces for commercial purposes. Entrepreneurs will not create new products if they are barred from capitalizing on their efforts.

The legislative efforts fall short of encouraging an open and adversarial online marketplace. What is needed is an approach specifically tailored to prevent platforms from using the CFAA as a weapon to hinder competition. One way to achieve this would be to establish a safe harbor from civil action for entities that are adversarially interoperating with large online platforms without causing damage to the existing platform.

Large platforms will claim that such a proposal creates a cybersecurity risk. However, the criminal provisions of the CFAA would still apply to any activity that might be covered by a safe harbor. In other words, nefarious hacking such as exfiltrating data, installing malware, or accessing trade secrets would still be illegal. Only building a product upon or complementary with an existing product would be granted protection from civil action. Indeed, the Department of Justice recently announced a major revision to its policy for prosecuting cases under the CFAA. The new policy explicitly states that “good-faith security research should not be

charged.”³⁸ It is not a stretch to similarly treat incorporated entities attempting to compete with large platforms and acting in good faith.

Another approach to creating such a safe harbor could be similar to the Platform Transparency and Accountability Act proposed by the Stanford Cyber Policy Center. One part of this proposal would grant journalists and researchers a safe harbor from civil liability for gathering information from online platforms so long as they take reasonable steps to protect the privacy of the platform’s users, avoid misleading users, and do not materially burden the platform’s operation.³⁹ Such a framework, in which policymakers articulate the “rules of the road” for good-faith interoperation could help spur a flourishing of competition in digital markets.

07 CONCLUSION

CFAA reform is not a silver bullet, correcting every problem facing digital markets. Big Tech companies will not open interfaces or welcome competitors with open arms; in fact, they are trending in the opposite direction. Lawmakers must still grapple with questions surrounding issues such as data privacy that adversarial interoperability alone is unlikely to address. But large online platforms should not be allowed to abuse the law to inhibit competition. Regardless of what other efforts might be necessary, eliminating a significant impediment to adversarial interoperability by reforming the CFAA is low-hanging fruit for lawmakers concerned with the dominance of Big Tech. ■

36 *Van Buren v. United States*, 593 U.S. ___, 141 S.Ct. 1648 (2021).

37 Augmenting Compatibility and Competition by Enabling Service Switching Act, S. 4309 and H.R. 3849, 117th Cong. § 2 (2021).

38 Press Release, Department of Justice Office of Public Affairs, Department of Justice Announces New Policy for Charging Cases under the Computer Fraud and Abuse Act (May 19, 2022), <https://www.justice.gov/opa/pr/departments-justice-announces-new-policy-charging-cases-under-computer-fraud-and-abuse-act>.

39 Tara Wright, *The Platform Transparency and Accountability Act: New legislation addresses platform data secrecy*, Stanford University Cyber Policy Center (December 9, 2021), <https://cyber.fsi.stanford.edu/news/platform-transparency-and-accountability-act-new-legislation-addresses-platform-data-secrecy>.

CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit [competitionpolicyinternational.com](https://www.competitionpolicyinternational.com) today to see our available plans and join CPI's global community of antitrust experts.

