Data is the oil of the twenty-first century and the technology companies that control this resource have become uniquely influential non-state actors. By tapping into an unlimited reservoir of user information, social media and digital communications companies have developed algorithms and targeted advertisements that influence the information and products its users consume. U.S.-based tech companies like Google, Facebook, Amazon, and Apple, among others, have become some of the most transformative and profitable companies in the world.

But the speed with which these companies have come to dominate our economic, social, and political lives has obscured their excesses. Thoughtful regulatory measures on these companies can give individuals more control over their digital lives and promote greater technological competition. Moreover, a well-regulated U.S. tech sector that safeguards the universality of a free and open Internet will sharply contrast the increasing number of restrictive Internet adaptations developing abroad.

DIGITAL MANIPULATION AND TECH COMPETITION
Social media platforms have not done enough to deter foreign and domestic actors from undermining trust in democracy and enflaming pre-existing divisions. In 2016, Russia weaponized social media to help elect Donald Trump and push the United Kingdom to exit the European Union. Using harvested personal information, political data-mining businesses like Cambridge Analytica have facilitated micro-targeted digital political campaigns. Bowing to mounting public pressure, some social media companies have taken steps to self-regulate. Facebook has introduced Off-Facebook Activity, a tool that allows user to view the personal data harvested from their browsing histories and barring Facebook from using it for targeted advertising. Additionally, Facebook, Twitter, and YouTube recently removed hundreds of Chinese accounts spreading disinformation about the ongoing protests in Hong Kong. While these are positive reforms, these platforms should begin to play a more proactive role in combatting disinformation and data abuse rather than reacting to on-going crises.

The dominance of a handful of U.S. tech companies is also beginning to stifle competition. The largest technology companies protect themselves by buying promising startups and folding them into their business or emulating their popular features. This lack of competition makes it difficult for consumers to hold tech companies accountable for major privacy failures.
THE U.S. REGULATORY LEADERSHIP VACUUM

Since their creation, the U.S. government has largely taken a laissez-faire approach toward regulating its technology giants. The Honest Ads Act and Bot Disclosure Accountability Act in the U.S. Senate would require technology firms to disclose advertising methods and limit the use of automation behind ad messaging on social media, but the latter was not enacted in the previous session of Congress and the former lacks sufficient support. Whereas the federal government’s anti-trust oversight remains lax, state legislatures have taken it upon themselves to protect their constituents’ digital information. Most significantly to date, California’s Consumer Privacy Act gives its residents more autonomy and insight into the use of their personal information online.

In the absence of U.S. leadership, the European Union has stepped up as the world’s leading big tech watchdog. Last year, the European Union adopted the General Data Protection Regulation (GDPR), which provides its citizens with tough privacy protections and enforces significant fines against technology companies that fail to meet regulations. EU member states have taken further steps to protect their citizens’ data. Germany recently blocked Facebook from pooling cross-platform data without user consent. In the United Kingdom, the Report of the Digital Competition Expert Panel called for closer examinations of tech mergers and encouraged large companies to share their data with smaller firms.

As Europe and the United States develop disparate approaches toward tech regulation, China has taken bold steps to define global digital norms. Modeled after Europe’s GDPR, Beijing’s privacy standard, the Personal Information Security Specification (“the Standard”), gives Chinese citizens a degree of control over their personal data while protecting the interests of its booming technology sector. Contradictorily, the Standard also establishes the principle of “data sovereignty” that specifies that all information of citizens must be stored in-country and can be accessed on-demand by the Chinese government. The digital dimensions of China’s Belt and Road Initiative, including fiber optic cables, 5G networks, and satellites, makes the prospect of Chinese data misuse abroad foreseeable.

Furthermore, China’s “Great Firewall” has become the global gold-standard of censorship and surveillance for other authoritarian countries. Beijing uses data gleaned from its tech giants to refine its vast domestic surveillance state, most glaringly on display in its Xinjiang province. The Chinese government uses a combination of facial recognition technology, cataloged biometric data, and artificial intelligence to surveil its Uyghur Muslim population. It is estimated that China has incarcerated 3 million Uyghurs in “political education” camps. Around the world, an increasing number of countries are embracing China’s vision for a tightly controlled Internet over the permissive American model. Already, 18 countries have purchased Chinese-made intelligence monitoring systems, and 36 have received training in censorship. Left unchecked, this
Orwellian technology will give authoritarian countries greater control over their citizens’ behavior and degrade the openness of the Internet.

**LEADING BY EXAMPLE ON TECH REGULATION**

The United States stands at a crucial intersection, with the current path leading toward more data manipulation, a permanent technological oligarchy, and a balkanized World Wide Web. The United States must change course and start leading this serious conversation.

Using Europe’s GDPR and California’s Consumer Privacy Act as a foundation, the United States should develop its own regulatory framework to manage its tech giants. In doing so, it can provide greater transparency to digital consumers and establish penalties against companies that enable the maligned use of users’ personal information. Citizens who access these platforms have a right to see which data-mining firms have made use of their online behavior and to identify the ultimate beneficiary of their information. Technology companies that monetize their users’ information should be required to submit their ads to a public archive that would enable private and public organizations to identify misinformation and influence campaigns in real-time. Large technology companies also should be encouraged to share a portion of their data with cities, promising tech startups, civic groups, journalism outlets, and research institutions. Under the control of a third-party trust, this data would be used in ways that involve and benefit citizens.

The United States also must revamp its anti-trust toolkit. Competition authorities should encourage greater watchfulness over corporate takeovers that could permanently damage innovation and consumer choice as well as over mergers involving massive quantities of user data. The government should push for measures that catalyze greater technological competition as well. A variable-compliance cost structure would avoid insulating the largest corporations from challenging platforms and promote a contest of ideas between startups and legacy tech companies. Additionally, compulsory contributions to state revenue would push tech companies to offer their services without advertisements. Congress could add a digital ad surcharge to the corporate income tax of the largest technology companies and state legislatures could adopt a sales tax on the revenue a company earns from the social media ads its residents view. This tax would incentivize the largest tech companies to offer ad-free subscriptions, find new revenue opportunities, and minimize the potential of malign influence on their platforms.

Finally, to reaffirm its place as a global technology leader, the United States must engage in global discussions to find common ground on digital norms and regulations. The United States should begin by adopting the privacy protection laws outlined in Europe’s GDPR and the private sector protections codified in China’s privacy specification. The United States also could become a party to the GDPR, enabling it to improve the agreement and promote stronger transatlantic
TO REAFFIRM ITS PLACE AS A GLOBAL TECHNOLOGY LEADER, THE UNITED STATES MUST ENGAGE IN GLOBAL DISCUSSIONS TO FIND COMMON GROUND ON DIGITAL NORMS AND REGULATIONS.

Encouragingly, G7 leaders endorsed a “Strategy for an Open, Free and Secure Digital Transformation” at the recent summit in France. To avoid further splintering the Internet, the U.S. government must lead these difficult discussions with allies and adversaries alike. Creating more shared databases for researchers with China and Europe would be a promising start. The United States must become an active participant in regulating its tech companies, not only for the sake of its citizens, but to preserve an open Internet and the international liberal order it leads.

CONCLUSION
Humans have regulated the ownership of private property for thousands of years, but we have limited experience regulating the ownership of personal data. To restore digital autonomy to its citizens and prove itself as a capable global leader in digital governance, the United States must do more to curb the harmful side effects associated with its tech giants. In doing so, it will make its Internet policies more attractive than the emerging authoritarian approaches towards the digital commons. If the United States fails to address this challenge head-on, it will inevitably lead to more data manipulation, ungovernable tech giants, and an increasingly fractured World Wide Web.

Bradley Honigberg is a social media and outreach coordinator with the Office of External Relations at CSIS.
ENDNOTES


15. Olaf Storbeck, "Germany Blocks Facebook from Pooling User Data without Consent, Financial Times, February 7, 2019, https://www.ft.com/content/3a0351b6-2ab9-11e9-88a4-c32129756dd8.


