MARCH 2025

NSI CYBER AND TECH CENTER

DATA AS A WEAPON: THE OVERLOOKED DOMAIN

By *Amy K. Mitchell*

CTC LAW AND POLICY PAPER

DATA AS A WEAPON: THE OVERLOOKED DOMAIN

THIS NSI LAW AND POLICY PAPER:

1 **EXAMINES** the intersection of privacy and data policy and their respective impacts on the American consumer.

2 **DETAILS** the domestic and national security implications of how consumer data is being used and may be used in the future.

3 **PROPOSES** policy recommendations to safeguard Americans from bad actors and adversaries of the United States.

ABOUT THE AUTHOR

AMY K. MITCHELL
Visiting Fellow at GMU NSI & Founding Partner at Kilo Alpha Strategies

Amy K. Mitchell is a founding partner at Kilo Alpha Strategies, bringing extensive national security and defense expertise from advising three Secretaries of Defense and leading strategic initiatives at the State Department. A former member of the Senior Executive Service, she was a Special Assistant to Secretary of Defense James Mattis and received the Distinguished Public Service Medal, the Pentagon's highest civilian honor. She has held key roles in government, public affairs, and Capitol Hill, shaping policy and communications on national security, veterans' issues, and global affairs. Currently, she is a Senior Fellow at George Mason University's National Security Institute and an advisor to several policy and veterans' organizations.

See page 12 for full bio.

CONTENTS

02 BACKGROUND

04 KEY ISSUES AT STAKE

06 AUTHOR’S VIEWS

07 ACTIONABLE RECOMMENDATIONS

10 ENDNOTES

BACKGROUND

INTRODUCTION

- **Digital Innovation is Outpacing Policy.** As a society, we are increasingly reliant on digital solutions in our personal and professional lives. Unfortunately, technology innovation and adoption continue to outpace public policy. One need only look to the Artificial Intelligence (AI) arms race, the legislative scramble to rein in American-owned social media companies such as Facebook (Meta), X (formerly known as Twitter), and YouTube, or the debate over Chinese-controlled TikTok.
- **Setting Guardrails Now.** Making major public policy shifts once the "train has left the station" are often expensive, distributive, and futile. With the renewed national focus on data and AI, now is the time to have the difficult discussions regarding the use of big data while policies, actions, and the ability to implement proactive "guardrails" remain within human control.

DATA AS A BUSINESS

- **Data is Big Business.** The global data market – which encompasses the ecosystem of data generation, collection, processing, storage, and exchange and includes the buying and selling of data by various stakeholders – is currently valued at over $160 billion USD and it is expected to balloon to at least $500 billion annually by the end of the decade.[1]
- **Every Click and Action is Recorded and Sorted.** Data that is collected is either stored for future use on a remote server (sometimes outside the United States)[2] or sold to marketing firms and others to enable curated experiences.[3] New entry points, such as facial and fingerprint scans on phones and bank accounts, create a digital trail of personally identifiable information (PII) including highly sensitive biometrics, which could be exploited for unscrupulous purposes in the future.
- **Seemingly Innocent Data is Being Collected.** Since data can be used to make life easier by increasing convenience, enhancing services, and providing personalized experiences, many Americans willingly share it through websites, social media, and virtual assistant devices such as Alexa – all without reading the lengthy terms and conditions in the agreements that accompany digital products and services.
  - Often, people do not realize that the large amounts of data they share through different forms of engagement may be used for nefarious means. These types of "innocent data" may include simple daily tasks, such as checking the weather forecast or sharing vacation photos on social media. As a result, the convenience of personalized recommendations, reminders, and remote devices almost always ensures that Americans

not only gloss over "opt-out" options – which allow individuals to prevent companies or organizations from collecting, storing, or using their personal data, but which are also time-consuming, confusing, and full of legalese – they forgo them.[4] Hitting accept has become the default, despite the accumulation of digital breadcrumbs that paint a vivid picture of habits and lifestyle choices that could be used by bad actors to impersonate and exploit individuals.

DATA AS A WEAPON

- **China's Global Data Play.** In 2020, reports detailed the People's Republic of China (PRC) wielding insidious influence within the UN Global Geospatial Knowledge and Innovation Center, a little-known UN bureau. Despite U.S. objections to the decision to locate the Center in China, construction on the new facility in Daqing has begun, thereby ensuring that much of the world's data, including census and health data, will flow into these new servers.[5] Further, there is no guarantee that this data will not be shared with or utilized by the PRC or China's People's Liberation Army (PLA) in the future.[6]
    - To expand its global influence, China also has been growing its Digital Belt and Road Initiative, which launched in 2015 and incorporates PRC initiatives aimed at collecting the data of individuals beyond its borders. Nations including Ecuador, Egypt, Malaysia, Nigeria, Pakistan, and Zambia,[7] among others, have signed contracts with the PRC to invest in and build smart ports and cities connected by Chinese-owned and operated Huawei 5G networks and underwater fiber-optic cables.[8] By establishing these infrastructure projects with built-in Huawei 5G capabilities, data from these projects can be sent back to servers in China to be saved indefinitely.
- **AI is Only as Good as the Data.** One of the biggest concerns regarding AI is the validity of the underlying data. AI models, especially those based on machine learning, rely on vast amounts of data to learn patterns and relationships and to deliver accurate decisions and results. Data must be "clean" – meaning true, accurate, and complete – to help ensure mis/disinformation from U.S. adversaries is flagged, disregarded, or eliminated in data processing.
    - For example, if "dirty" or false data is injected into AI platforms such as ChatGPT or Facebook, the ability to rewrite events, histories, and facts will become commonplace, creating a world where everyone and everything is questioned. This tactic is exemplified by Russia's information warfare campaigns in its war on Ukraine, unfortunately, to great effect.[9] This data, once injected into a system, is extremely costly and difficult to remove.
        - Federal agencies such as the Department of Defense have recently updated their data and AI policies[10] to emphasize the importance of human oversight and clarify what it deems "responsible AI."[11] This means that, despite the speed of AI, a human will always be at the end of the DoD decision tree in making final recommendations, ensuring a safer approach.

KEY ISSUES **AT STAKE**

DOMESTIC CONCERNS

- **Public Safety.** The increased use of and advancements in AI have raised concerns about its misuse, including its role in doxing and false flag information, and its potential harm to Americans.
  - For example, advancements in facial recognition technology have contributed to a rise in doxing and false flag information. In regard to doxing, facial recognition tools can scan publicly available images on social media or surveillance footage to identify individuals. Once identified, an individual's personal information (e.g., name, location, employment details) can be shared publicly in an effort to harass or intimidate.
    - There have been instances where facial recognition technology was used to identify and dox individuals involved in protests, activism, or reporting on contentious issues.[12]
  - Further, facial recognition technology can be combined with deepfake technology to create false flag information. In these cases, highly convincing fake videos or images are manufactured to appear as though an individual is involved in actions or making statements they never actually did.
    - Due to these dangers and the ability of individuals to use these technologies to perpetrate crimes, some U.S. law enforcement no longer use facial recognition technology to identify suspects, and in numerous jurisdictions, use of the technology has been outright banned.[13] While some advances in technology, like DNA forensics, have benefited law enforcement and even led to a decrease in wrongful convictions, other technologies, such as facial recognition, have had the opposite effect and have created a new class of crimes.
- **Consumer Protection.** While more companies are offering tools to increase convenience or lower end-user costs, these tools often collect some of the American consumer's most personal data and raise significant privacy concerns.
  - For example, in addition to new technologies being built into vehicles today – all of which collect data – drivers can also voluntarily use "safe driving" apps offered by many car insurance companies. These apps continuously track routes, habits, cell phone use, and mileage, ostensibly to help lower insurance costs.[14] While these types of safe driving discount programs are seemingly well-intentioned, insurance companies now have access to immense amounts of personal data, which could potentially be shared with third parties, without the full knowledge or consent of the driver.
  - Further, while these safe driving apps are positioned as voluntary, personal economic considerations frequently drive consumers into sacrificing personal data for cheaper insurance policies. This type of collection is happening across multiple industries. In one notable example, two teenagers were able to use AI modeling to predict the result of an election within hundreds of votes using publicly available census data of the residents of a New York district.[15]

INTERNATIONAL CONCERNS

- **Adversarial Technology at Home.** Americans continue to use a wide range of products and technologies made by adversarial nations, raising additional privacy and security concerns. For example, foreign-made devices can collect and send sensitive personal data of Americans to servers in other countries, some of which have laws requiring companies to provide data to their governments upon request.[16] Products ranging from high-tech electronics – such as drones (the majority of which are made by China's DJI)[17] – to seemingly harmless products such as a popular dog treat dispenser and camera (also from DJI), are readily available to Americans.
- **Adversarial Technology in Public.** The use of adversarial tech extends beyond American consumers and into U.S. federal and state government agencies. For example, an estimated 600,000 Hikvision CCTV cameras, which are manufactured in China, are in use across the U.S., with more than 100 U.S. state and city governments using surveillance technology made by Hikvision and Dahua Technology, another Chinese company, at locations including public schools and police departments.[18] Hikvision's facial recognition technology has been credibility accused of complicity in the CCP's genocide against the ethnic Uyghur population in Xinjiang.[19] While Hikvision has been sanctioned by numerous U.S. government agencies, its technology remains on hundreds of thousands street corners, in stores, and in public venues across the nation, collecting data on everyday Americans.

» **"AN ESTIMATED 600,000 HIKVISION CCTV CAMERAS, WHICH ARE MANUFACTURED IN CHINA, ARE IN USE ACROSS THE U.S., WITH MORE THAN 100 U.S. STATE AND CITY GOVERNMENTS USING SURVEILLANCE TECHNOLOGY MADE BY HIKVISION AND DAHUA TECHNOLOGY, ANOTHER CHINESE COMPANY, AT LOCATIONS INCLUDING PUBLIC SCHOOLS AND POLICE DEPARTMENTS."**

AUTHOR'S **VIEWS**

POLICYMAKERS NEED TO ACT

- **State Legislatures are Starting to Act.** In recent years, 15 states – including California, Florida, and Texas – have enacted legislation to protect consumer data privacy.[20] Some state laws now provide child protections, rights to access, correct, and delete personal data, and restrictions on "sensitive data."[21] Additionally, more than 30 state legislatures have taken action to restrict TikTok, the most scrutinized foreign app, for its potential to collect and misuse user data.[22]
- **The Federal Government has been Slow to Act.** At the federal level, despite its latest effort to breakup TikTok, the government continues to rely on outdated legislation, such as Section 230 of the Communications Act of 1934[23] and the Privacy Act of 1974 for data privacy and related industry responsibilities. Meanwhile, multiple federal agencies from the Federal Communications Commission (FCC) to the Cybersecurity and Infrastructure Security Agency (CISA) to the Department of Health and Human Services, are implementing piecemeal executive policies without a dedicated enforcement agency in the lead.
- **Technology is Outpacing Congressional Action.** With stalled initiatives like the American Privacy Rights Act of 2024[24] and the RESTRICT Act,[25] it is clear that Congressional legislators are scrambling to respond to the growing calls for data protection.[26] To date, Congress has been unable to keep pace with technological advances or to install guardrails that protect Americans and U.S. national security.

INDUSTRY HAS A ROLE TOO

- **Industry's Role in Data Protection.** While the tech industry has driven innovation and profited from data, it too has joined the growing chorus of voices expressing concern. If these companies are serious about reform, they must lead on the ethical and moral implications of data and privacy within their own technology, independent of any executive or congressional action.
- **Taking a Lesson from Consumer Protection.** Technologies that raise privacy concerns and threaten national security should be treated like processed food, which utilizes mandatory labeling to inform consumers about potential health and safety impacts. Problematic technologies – especially those which collect personal data – should be held to similar standards. If guns are eligible for warning labels[27] then apps – that studies show are detrimental not only to the mental health of its users, but also control huge repositories of personal data – should also carry warnings. A simple warning label could read: "Use of this product or service may provide information to adversaries of the United States that may be used to harm you and/or members of your family."

ACTIONABLE **RECOMMENDATIONS**

1 EXECUTIVE ACTION

- **Prioritize Data.** The executive branch must ensure federal agencies, particularly those in the national security establishment, with tools such as trusted systems, modernization, and staff with the appropriate skill sets to address the "deluge of data."[28] If agencies lack these tools, it is the responsibility of the White House to prioritize these needs in the next federal budget. This requires doubling the current amount of allocated funding – $75 billion – to keep pace with adversaries.
- **Break Down the Silos.** Coordination among federal agencies must be streamlined. A centralized office should coordinate federal efforts until Congress designates an appropriate lead agency. An Executive Order could direct the FCC, given its broad mandate, to initiate an inter-agency study on all data touchpoints across the U.S. government. This taskforce should deliver its findings and recommendations to the National Security Council within six months. Data privacy should also be elevated to the level of NSC's Deputies Committee, due to its critical role in national security.
- **The U.S. Consumer is the Innocent Party.** Finally, the executive branch has an obligation to keep the public better informed about how adversaries are exploiting Americans' most personal data. Occasional FBI press conferences are not enough. Last year alone, nearly 1 million consumers' personal data was compromised, costing more than $10 billion.[29] Americans need better mechanisms to report these incidents and secure redress, particularly when breaches are the result of government or industry failures. The FBI is the lead on this issue, but it too has been inundated with data, and complaints, which requires an increase in dedicated staff and resources to investigate these crimes.

  Consumers should not have to rely solely on trial lawyers and class-action lawsuits to reclaim losses; instead, a structured system should ensure they have rights and recourse, which will involve expanded cybercrime units and an increase in federal investigators to actually apprehend perpetrators and hold them accountable.

> "CONGRESS HAS BEEN UNABLE TO KEEP PACE WITH TECHNOLOGICAL ADVANCES OR TO INSTALL GUARDRAILS THAT PROTECT AMERICANS AND U.S. NATIONAL SECURITY."

2 LEGISLATIVE ACTION

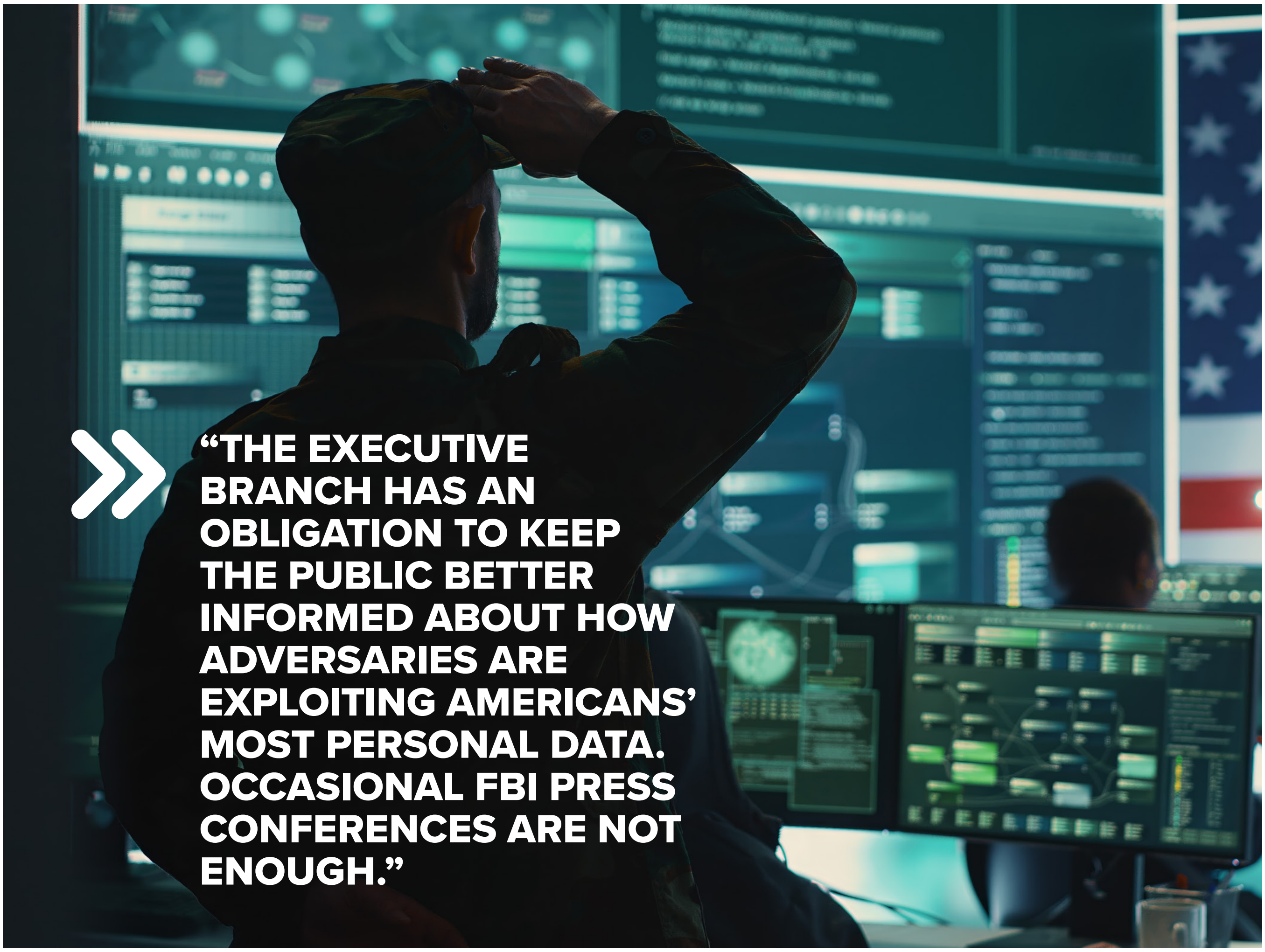
- **The Time to Act is Now.** Addressing the national security risks posed by emerging technologies and data collection demands expanding, updating, and closing loopholes in current federal laws.[30] The American Privacy Rights Act of 2024 is a vital step. but if a comprehensive bill cannot be passed, Congress should enact targeted measures to fill critical gaps, such as enabling consumers to delete their own data and imposing time-limited retention of personal data with meaningful, monetary penalties for non-compliance.
- **Secure Government Systems.** Legislative action bolsters cybersecurity protections to prevent adversaries like CCP from exploiting and collecting open-source intelligence (OSINT) of key government personnel. This includes additional funding for the FBI to investigate such cyber incursions, enhance cybersecurity protections, and train federal employees. Many federal IT offices are not equipped, nor staffed, to protect against persistent threats from U.S. adversaries, underscoring the need for stronger safeguards.
- **Restore Consumer Rights.** Most importantly, consumers should be in control of their data, including a shift from the current opt-out approach to an opt-in model. This would allow individuals to access and delete their personal information more easily. Lobbyists should not dictate the use, storage, or sale of Americans' data – consumers should have the power to make these choices themselves.

3 INDUSTRY

- **Industry Must Self-Correct.** Industry has played a role in creating this data privacy crisis by opening Pandora's box, and therefore should be a part of the solution. A review of European privacy frameworks could provide valuable insights for a consumer-focused approach in the U.S.[31] Industry leaders must adopt clear, consumer-friendly data protection policies that can be easily understood in under a minute or less, rather than burying extensive use of personal information in lengthy indemnity clauses. If industry fails to lead on this issue, Congress must step in with legislation that ensures transparency and accountability. This should also include financial penalties for abusing U.S. citizen data.
- **Plan for the Future.** An industry-led data task force, akin to the AI taskforce, should be established, comprising of industry leaders, political scientists, statisticians, and economists to bring a comprehensive perspective. This task force should have two mandates: to dismantle bureaucratic barriers and examine existing practices and to anticipate the rapidly changing geopolitical landscape by providing recommendations for protecting consumers and critical infrastructure. Congress should set clear deadlines for the task force to present a framework that balances legislation, policy, and consumer rights in a data-driven world where information can be weaponized.

CONCLISION

- **Data as a Battleground.** Data is quickly emerging as a critical domain in modern warfare. Policymakers must mitigate risks posed by captured, stolen, or falsified data, which could have real national security consequences.
- **Be Wary of Technological Evolution.** Banning certain technologies may only lead to the creation of alternatives. Policymakers must stay vigilant when it comes to the misuse of Americans' data. As the potential of a change in ownership or the shuttering of TikTok continues to be debated, ByteDance has already launched Red Note and Lemon8 as its successor.[32]
- **Act Strategically and Swiftly.** The scale and interconnected nature of data require policymakers to adopt faster, more strategic solutions. Traditional policy approaches may not be sufficient to stem the tide of unregulated data flows, which could become one of the most dangerous digital threats of the 21st century.



> **"THE EXECUTIVE BRANCH HAS AN OBLIGATION TO KEEP THE PUBLIC BETTER INFORMED ABOUT HOW ADVERSARIES ARE EXPLOITING AMERICANS' MOST PERSONAL DATA. OCCASIONAL FBI PRESS CONFERENCES ARE NOT ENOUGH."**

ENDNOTES

[1] Richard Johnson, “Big Data Market and Region Forecast, 2022 – 2030,” Acumen Research and Consulting, December 15, 2022, https://www.globenewswire.com/en/news-release/2022/12/15/2575145/0/en/Big-Data-Market-Size-Set-to-Achieve-USD-473-6-Billion-by-2030-growing-at-12-7-CAGR-Exclusive-Report-by-Acumen-Research-and-Consulting.html.

[2] Giorgio Bonuccelli, “Cloud Vs Server: Learn the Key Differences and Benefits,” Parallels, March 9, 2022, https://www.parallels.com/blogs/ras/cloud-vs-server/.

[3] Nik Froehlich, “The Truth In User Privacy And Targeted Ads,” *Forbes*, February 24, 2022, https://www.forbes.com/sites/forbestechcouncil/2022/02/24/the-truth-in-user-privacy-and-targeted-ads/?sh=6e45bd35355e.

[4] Lee Rainie, “Experts Say the ‘New Normal’ in 2025 Will Be Far More Tech-Driven, Presenting More Big Challenges,” Pew Research Center, February 18, 2021, https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2021/02/PI_2021.02.18_New-Normal-2025_FINAL.pdf.

[5] Claudia Rosett. “China Uses the U.N. to Expand Its Surveillance Reach,” *Wall Street Journal*, October 7, 2020, https://www.wsj.com/articles/china-uses-the-u-n-to-expand-its-surveillance-reach-11602111456.

[6] Rosett, “China Uses the U.N. to Expand Its Surveillance Reach.”

[7] Joshua Kurlantzick and James West, “Assessing China’s Digital Silk Road Initiative,” Council on Foreign Relations, https://www.cfr.org/china-digital-silk-road/.

[8] Kurlantzick and West, “Assessing China’s Digital Silk Road Initiative.”

[9] Catherine Belton, “Kremlin Runs Disinformation Campaign to Undermine Zelensky, Documents Show,” *Washington Post,* February 16, 2024, https://www.washingtonpost.com/world/2024/02/16/russian-disinformation-zelensky-zaluzhny/.

[10] U.S. Department of Defense, *DoD Directive 3000.09: Autonomy in Weapon Systems*, approved by Kathleen H. Hicks, January 25, 2023, Office of the Under Secretary of Defense for Policy, https://www.esd.whs.mil/DD/.

[11] Jaspreet Gill, “DoD’S Update to Autonomous Weapons Policy Accounts for AI’S ‘Dramatic’ Future Role,” *Breaking Defense*, January 25, 2023, https://breakingdefense.com/2023/01/dods-update-to-autonomous-weapons-policy-accounts-for-ais-dramatic-future-role/.

[12] Joseph Cox, “Taylor Swift Facial Recognition TikTok Deletes Videos After 404 Media Investigation,” *404 Media*, October 2, 2023, https://www.404media.co/taylor-swift-facial-recognition-tiktok-removes-videos/.

[13] “Ban Facial Recognition,” Fight For the Future, https://www.banfacialrecognition.com/map/.

[14] Omri Ben-Shahar, “Privacy Protection, At What Cost? Exploring the Regulatory Resistance to Data Technology in Auto Insurance,” Journal of Legal Analysis, Volume 15, Issue 1, 2023, Pages 129–157, https://doi.org/10.1093/jla/laad008.

[15] Reed Albergotti, “No people, no problem: AI chatbots predict elections better than humans,” *Semafor,* September 20, 2024, https://www.semafor.com/article/09/20/2024/ai-startup-aaru-uses-chatbots-instead-of-humans-for-political-polls.

[16] Reuters, “US to Propose Ban on Chinese Software, Hardware in Connected Vehicles, Sources Say,” September 22, 2024, https://www.voanews.com/a/us-to-propose-ban-on-chinese-software-hardware-in-connected-vehicles-sources-say/7794115.html.

[17] Laura Dobberstein, “US Agencies Warn Made-in-China Drones Might Help Beijing Snoop on the World,” *The Register*, January 19, 2024, https://www.theregister.com/2024/01/19/drone_cisa_fbi/.

[18] Nuzigum Setiwaldi, “Surveillance Tech Series: Hikvision’S Links to Human Rights Abuses in East Turkistan,” Uyghur Human Rights Project, October 17, 2023, https://uhrp.org/report/hikvisions-links-to-human-rights-abuses-in-east-turkistan/#:~:tex-

t=More%20than%20600%2C000%20Hikvision%20cameras,%2C%20Los%20Angeles%2C%20and%20Houston.&text=More%20than%20100%20US%20state,schools%20and%20police%20departments%2C%2023.

19 Al Jazeera, “US Sanctions Chinese Firms over Alleged Repression of Uighurs,” *Al Jazeera*, March 29, 2023, https://www.aljazeera.com/economy/2023/3/29/us-sanctions-chinese-firms-over-alleged-abuses-of-uyghurs.

20 Jennifer G. Prozinski and Imani T. Menard, “New State Data Privacy Laws in 2024,” Venable LLP, February 29, 2023, https://www.venable.com/insights/publications/2024/02/new-state-data-privacy-laws-in-2024#:~:text=There%20are%20now%2015%20states,Texas%2C%20Utah%2C%20and%20Virginia.

21 Gibson Dunn Lawyers, “U.S. Cybersecurity and Data Privacy Outlook and Review – 2023,” Gibson Dunn, January 30, 2023, https://www.gibsondunn.com/us-cybersecurity-and-data-privacy-outlook-and-review-2023/.

22 Sapna Maheshwari and Amanda Holpuch, “Why the U.S. Is Forcing TikTok to Be Sold or Banned,” *New York Times*, April 26, 2024, https://www.nytimes.com/article/tiktok-ban.html#:~:text=But%20students%20often%20just%20switch%20to%20cellular%20data%20to%20use%20the%20app.&text=In%20May%202023%2C%20Gov.,legislation%20violated%20the%20First%20Amendment.

23 Congressional Research Service, *Section 230: A Brief Overview*, February 2, 2024, https://crsreports.congress.gov/product/pdf/IF/IF12584.

24 Committee Chairs Maria Cantwell and Cathy McMorris Rodgers, “Committee Chairs Cantwell, McMorris Rodgers Unveil Historic Draft Comprehensive Data Privacy Legislation,” April 7, 2024, https://www.commerce.senate.gov.

25 Congressional Research Service, *RESTRICT Act*, Congress.Gov, March 7, 2023, https://www.congress.gov/bill/118th-congress/senate-bill/686.

26 Brendan Bordelon, “Congress Goes Wobbly on TikTok,” *Politico*, March 31, 2023, https://www.politico.com/news/2023/03/31/senate-tiktok-bill-restrict-act-00089926.

27 George Petras, “Gun Violence Is a Public Health Crisis, Surgeon General Says: A Look at the Statistics,” *USA Today*, January 11, 2025, https://www.usatoday.com.

28 Julian E. Barnes, “China Investing in Open-Source Intelligence Collection on the U.S.,” *New York Times*, June 1, 2023, https://www.nytimes.com/2023/06/01/us/politics/china-us-open-source-intelligence.html?unlocked_article_code=UhSicPweZ-rboQHA0a94sqTGXoEPsrC9eI8rJNP7IghRQfsgalJWe2lmj2Z-BqklcZC2QIpZub1xNRtxAY8FZZrGWElYCdK7OOQkqMSdg8Rn-n30oyEiWZwUdHorTeAWsRAlNvy_jUoDL0JFZgrY6rxfsFLuvh7Ucxjy_HLa7KgcDTm-n5D2LuT3bVJermVxXho9DKWZGWix857_CVuBOl6Qf4dQ0z2wjQNL86HrV1lH7bbPPHDQJq8X9ZZoQwDLe8GAlykup-Ce6r_QxCGj2tv9EsqJb1PMxVzSPsNOMe5NN6T1D-qkrAhrxL2LzLNgQ96dxUFVj9t9eM94AgdgWIZTwhWpg01Fj7rMz7RQzqB6A&smid=em-share.

29 Federal Bureau of Investigation, *2023 Internet Crime Report*, January 2024, https://www.ic3.gov.

30 Dan Smith, “The CFPB Has a Data Privacy Blind Spot,” *The Hill*, January 27, 2023, https://thehill.com.

31 Fredric D. Bellamy, “U.S. Data Privacy Laws to Enter New Era in 2023,” *Westlaw Today*, January 12, 2023, https://www.reuters.com/legal.

32 Eric Cheung, Joyce Jiang, and Hassan Tayir, “The Great Social Media Migration: Sudden Influx of US Users to RedNote Connects Chinese and Americans Like Never Before,” CNN, January 15, 2025, https://www.cnn.com/2025/01/14/tech/rednote-china-popularity-us-tiktok-ban-intl-hnk/index.html.

ABOUT THE AUTHOR

AMY K. MITCHELL

Senior Fellow at GMU NSI & Founding Partner at Kilo Alpha Strategies

Amy K. Mitchell is a founding partner at Kilo Alpha Strategies. She brings extensive national security and defense experience to the firm having advised three Secretaries of Defense and several large defense contractors. Her unique understanding of U.S. national security and foreign policy interests provides companies with high-level insights and counsel.

Previously, Ms. Mitchell served as the Chief of Staff and Senior Advisor for the Office of Global Women's Issues at the State Department, where she advised the Department's senior leadership on strategic diplomatic initiatives, concentrated on the Indo-Pacific. She represented the office in interagency policy processes, bilateral and multilateral diplomatic engagements, and drove implementation of key policy decisions on China, Sudan, Sri Lanka, and other priority contexts. A member of the Senior Executive Service, she was also the Special Assistant to Secretary of Defense, General James Mattis. She advised the Secretary on public diplomacy and advanced the Department's critical mission of forging international partnerships and oversaw all high-level engagements and events. She was awarded the Distinguished Public Service Medal for her service, the Department's highest civilian honor.

Ms. Mitchell also has extensive Capitol Hill and public relations experience creating and executing a variety of public facing campaigns to inform veteran and military communities, as well as the public, including as the vice president of communications at National Review; vice president of public affairs at the United Service Organizations (USO); and as the director of communications at the House Committee on Veterans' Affairs.

Under President George W. Bush, she served at the Department of Defense as the Director of Special Projects, overseeing the Department's Wounded Warrior outreach efforts and supported the unveiling of the September 11 Pentagon Memorial. Ms. Mitchell's international relations career began as the deputy director of public relations at the G8 Summit in 2004 in Sea Island, Georgia. She is a graduate of the University of California at Santa Barbara.

Ms. Mitchell is currently a Senior Fellow at George Mason University's National Security Institute, a Non-Resident Senior Fellow at New Lines Institute; serves on the advisory board of the Vandenberg Coalition; is a member of the U.S. Global Leadership Coalition Foreign Policy Study Group; a strategic consultant to several military and veterans service organizations; and is on the board of Eagle Online Academy. She has appeared on Voice of America and Scripps News, and she has written numerous articles for The National Interest, Foreign Policy, and The Hill, among other publications.

TITLE RED HAT ENTERPRISE LINUX SERVER (2.6.32-696
ROOT (HD0,0)
KERNEL /VMLINUZ-2.6.32-696.6.3.EL6.X86_64 RO ROOT
ANG=EN_US.UTF-8 RD_LVM_LV=OS_VG/SWAP_01_LV
OT_LV KEYBOARDTYPE=PC KEYTABLE=US RD_NO_DM
ADLINE TRANSPARENT_HUGEPAGE=NEVER DEBUG
LV=OS_VG/ROOT_LV KEYBOARDTYPE=PC KEYTABLE=US
TITLE RED HAT ENTERPRISE LINUX SERVER (2.6.32-573.1.1
ROOT (HD0,0)
KERNEL /VMLINUZ-2.6.32-573.1.1.EL6.X86_64 RO ROOT
N_US.UTF-8 RD_LVM_LV=OS_VG/SWAP_01_LV RD_NO_MD
DTYPE=PC KEYTABLE=US RD_NO_DM ELEVATOR=NOOP
OARDTYPE=PC KEYTABLE=US RD_NO_DM ELEVATOR=DEADLINE

NSI | THE NATIONAL SECURITY INSTITUTE
At George Mason University's Antonin Scalia Law School

THE NATIONAL SECURITY INSTITUTE
Antonin Scalia Law School | George Mason University
3301 Fairfax Dr., Arlington, VA 22201 | 703-993-5620

NATIONALSECURITY.GMU.EDU