Cybersecurity Law Report

cslawreport.com

Oct. 11, 2023

Artificial Intelligence

Shaping AI Policy to Address Risks to U.S. Citizens and National Security

By Evelyn Remaley, *Wilkinson Barker Knauer LLP*

For new AI technologies where both the risks and rewards are still emerging, policymakers struggle to forge guidelines that will ensure consumer and national security protections while permitting innovation to thrive. Some are rushing to stave off what is perceived as a machine-led, dystopian future where Big Brother reigns and privacy is non-existent.

The future of the global economy and answers to the world's problems will be driven by data and data analytics, with AI and machine learning playing an outsized role, along with quantum computing as it continues to advance. AI gives technologists and innovators the ability to use the precision, reach and predictability of data to improve the ability to achieve autonomy for systems such as automobiles, drones and aircraft, and improve the ability to correlate factors to solve complex problems.

It is critical that future AI systems have built-in transparency and accountability mechanisms from the outset to ensure that risks related to bias, safety, discrimination and national security can be managed. However, bans on AI or "trigger regulation" will only put the U.S. behind in the global marketplace. Misaligned policy could also impact the quantum race and other emerging tech areas.

This article examines the technological shift and its impact in the U.S. In particular, it details three specific AI-driven risk scenarios involving sensitive data that are keeping policymakers up at night, as well as pending and proposed policy responses that are being considered to address those risks. Finally, it recommends nine guiding principles for data integrity in the age of AI, including building consensus around voluntary principles to safeguard market potential and protect consumers.

See "Takeaways From the New Push for a Federal AI Law" (Oct. 26, 2022).

Technological Shift Requires Safeguards

Technology advances – such as AI, machine-based learning, advanced analytics and eventually quantum computing advances – only make sensitive personal data easier to mine and patterns more discernable, enabling the targeting of individual Americans and impacting their collective security interests.

Impact of AI on Sensitive Data and National Security

There is an understanding within the national security community of the U.S. government that a repository of seemingly mundane personal data, in the aggregate, can present great risk simply by the amount of insight it may provide into an individual's economic, social, religious, or health habits and preferences, among other factors.

When data is enhanced by the predictive power of AI systems, U.S. citizens may be subject to fraud, exploitation and strategic disinformation from the country's adversaries. That risk is orders of magnitude higher if the AI infrastructure and/or data sets are owned, controlled or influenced by a foreign adversary government.

Counterintelligence is one of the largest risks of U.S. data exposure seen by policymakers, but the risks are much broader. Newly emerging risks such as deepfakes, algorithmic influence and online radicalization present new vectors for influencing the security of U.S. citizens. The impacts on children of data manipulation and exposure can be life threatening, as can impacts on democratic processes.

U.S. Government Acknowledgement of the Risk

In 2019, the Trump Administration declared a national emergency in response to the Information and Communications Technology and Services (ICTS) Supply Chain and called out several foreign adversaries in relation to that threat to include the People's Republic of China, Russia, Iran and North Korea. China and Russia view critical infrastructure supply chains as a key vector for gaining leverage during times of crisis. Having extensive control over a country's ICTS infrastructure – be that through investment or the provision of equipment or software – presents many avenues to restrict, deny or manipulate what individuals may or may not see online; restrict or deny advancements in ICTS technology and security fixes; restrict or deny access to ICTS technology; and use the technology as a vehicle to conduct kinetic effects.

With the risk of data exposure heightened by AI, the U.S. government is concerned about scenarios where so much detail is known about a person – or about organizations' trade secrets or national security – that the ability, through subtle or subversive methods, to manipulate, steal, sabotage, blackmail or influence will become universal, and perhaps even undetected by Americans. In 2021, the Biden Administration's Executive Order (EO) 14034, Protecting Americans' Sensitive Data From Foreign Adversaries, identified this threat, but with express acknowledgement that additional action would be required.

As a follow up to EO 14034, the President took to the press with an op-ed in the Wall Street Journal calling on Congress to come together to finally tackle privacy as a bipartisan issue. Months later, particularly with the rapid-fire public debut of generative AI, there is an onslaught of AI-specific policy and legislative proposals primarily under the auspices of consumer protection.

Encryption Not Enough

Some view the threat from foreign adversaries as somewhat diminished since much of the data shared online is encrypted. But the national security community is already looking ahead to a time when the U.S.'s current encryption approaches may not be enough to withstand the powerful computing and mathematical abilities of future quantum systems. U.S. policymakers believe that large stores of encrypted data are currently being collected by adversaries for decryption using quantum systems. To actualize this position, policymakers point to documented examples of malicious cyber activity where U.S. data has been collected by misrouting or exfiltration techniques, leaky code, or foreign owners that have an obligation to share data in their possession with foreign governments without being subject to the U.S. rule of law.

Need for Legal Framework

The U.S. government must adopt a framework for protecting sensitive data in an AI-fueled environment that does not unduly diminish the benefits that data innovation and AI can provide. The next wave of innovation in the tech sector will be driven largely by various forms of data (*e.g.*, financial, health, consumer). To maintain its leadership across the global digital economy, U.S. industry and government should be thinking strategically about how to introduce principles that foster domestic innovation and global cooperation, not inhibit it. One of those strategies certainly involves the global industry-led standards development process to ensure interoperability, but there are other cooperative measures that should be explored as well.

The following discussion provides insight into the evolving AI risk space impacting the sensitive data of U.S. citizens and offers a set of mitigation principles for safeguarding that data while continuing to foster a vibrant global digital marketplace.

See Cybersecurity Law Report's three-part series on new AI rules: "NYC First to Mandate Audit" (Jun. 15, 2022), "States Require Notice and Records, Feds Urge Monitoring and Vetting" (Jun. 22, 2022), and "Five Compliance Takeaways" (Jul. 13, 2022).

Three Risk Scenarios Enhanced by the Misuse of AI Technology

Scenario One: Mobile App Subject to Control by Foreign Adversary

In this scenario, a private corporation with ties to a foreign adversary provides communication services in the U.S. The app operates in a way to encourage Americans to widely use the app and to share sensitive data with the app, such as preferences, financial information and other personal details that are either overt or that can be discerned from the user's activity on the app. The data can be used to build a unique profile of the user and analyzed to determine potential options for influencing the user. Once the app becomes “sticky,” users may be reticent to leave the app and the data they have created there, even if they believe the app may be exploiting their data, mining it or sharing it with external governments without process. Once trust is established, the app becomes a possible vector for surveillance and disinformation on a large scale, especially fueled by AI and machine learning tools that are constantly developing more sophisticated ways to appeal to the app’s users.

Opportunities for Exploitation

The opportunities for exploitation in this scenario are extensive. The app provider could exfiltrate user data to foreign entities unbeknownst to users and may even store data in jurisdictions that offer diminished privacy protections. The app provider has exposure to potentially millions of users with knowledge of those individuals’ preferences and biometric information, as well as health, financial and family associations. The app provider could misroute data where it could be captured by foreign adversaries. The sensitive data can be stored by the foreign adversary and mined for national security secrets and/or preserved to allow for future analytics as AI and quantum technologies continue to advance.

Risks

The app provider could control or sabotage physical devices through the app, conduct mass surveillance, profile and target national security personnel, and conduct propaganda/social conflict campaigns as well as psychological manipulation. The app provider and the foreign adversary could use disinformation, deepfakes and blackmail to conduct targeted or wide-scale influence operations.

Scenario Two: Undersea Cables/Data Centers Subject to Control of Foreign Adversary

In this scenario, U.S. sensitive data is exchanged over undersea cables that are subject to the control of a foreign adversary. A U.S. provider may have a partnership with a foreign provider to ensure they can land the cable on foreign soil. The provider would also need to either operate a data center in that country or contract with an entity in that country for data center services. Once U.S. data transverses beyond the U.S. cable provider, U.S. law no longer applies to protect the data. In another related scenario, a provider that has been designated as high risk, for example listed on the FCC’s Covered List, may operate data centers in the U.S. without being subject to FCC restrictions.

Opportunities for Exploitation

Foreign adversaries have the opportunity to misroute or capture the data flowing over the cable at exchange points and/or data centers located in the foreign jurisdiction, especially if the jurisdiction is a foreign adversary. U.S. providers may lose insight into any downstream misrouting or mishandling of data once they exchange traffic with foreign peers or routing partners. In certain foreign jurisdictions, providers may be required to provide government access to data without legal process. In the U.S. data center example, the data center subject to the control of a foreign provider may have the ability to divert data to the foreign adversary and shield certain activity by foreign adversaries from U.S. law enforcement. These partners and providers may have the opportunity to introduce risks into the infrastructure at any time through cybersecurity updates or patches. Through the use of AI and other data management techniques, they could impact the integrity of the data or disrupt the intended flow of the data.

Risks

Foreign adversaries can mine U.S. sensitive data through these commercial relationships; create profiles of individual Americans, including U.S. security personnel; use AI to conduct espionage and theft of intellectual property; and conceal data or communications occurring between the U.S. and foreign entities from law enforcement.

Scenario Three: AI Data Sets and Algorithms Designed and Controlled by Foreign Adversary That Presents Safety or Security Risk

In this scenario, a foreign adversary applies AI to infrastructure control systems (*e.g.*, energy, transportation, drug testing/manufacturing, medical diagnosis) to improve efficiency and accuracy.

Opportunities for Exploitation

It is not yet clear how commercial AI technologies will be used in certain high-risk sectors such as transportation, smart cities, drone operation, energy production or management, and medicine. In these highly regulated industries where data manipulation could lead to life and limb consequences, it is important to ensure that AI systems, algorithms and devices are free from foreign adversary influence or control. Just as the U.S. government is cautious of certain foreign investments in these high-impact industries, it is also critical for the U.S. to examine AI governance in these sectors.

Risks

Risks are extensive and far reaching to include disruptions that threaten the physical safety of Americans.

See “Innovation and Accountability: Asking Better Questions in Implementing Generative AI” (Aug. 2, 2023).

Nine Principles to Guide Data Integrity in the Age of AI

Companies are deploying AI systems at a rapid pace to benefit from the technology’s efficiency and accuracy. These AI systems are being deployed across varying sectors, sometimes without an assessment of risks. Concurrently, the U.S. government has been taking an incremental approach to developing guidelines for AI systems, including voluntary commitments from AI creators and a draft code of conduct with international partners. It has also published two foundational policy documents, the National Institute of Standards & Technology's (NIST's) AI Risk Management Framework, and the AI Bill of Rights, while working to finalize a comprehensive AI Executive Order.

While the U.S. government pursues this incremental approach, the European Union is forging ahead on the development of AI regulation through its AI Act. Multinational companies that are seeking harmonized AI policies across the globe see an international race developing to establish AI standards and are concerned that strict regulatory requirements that limit innovation and experimentation will become the norm. Although many see a long-term path to regulation, they prefer voluntary approaches during the emergent commercial phase, and guidelines driven by risk before the promulgation of prescriptive regulation. As the E.U. nears completion of the AI Act, industry and global governments will be forced to make decisions regarding conformity to these rules, which can limit U.S. industry's ability to lead on global AI standards development and impact the global market for American AI innovation.

On risks to sensitive data and national security, the U.S. may still have the opportunity to lead the AI global policy conversation by forging agreement on common principles. Companies developing or adopting AI into their products and services can also help protect the global market for AI innovation by also driving consensus around these principles.

The following core concepts will be key to operationalizing an actionable, comprehensive regime that governs both AI systems and data integrity.

1) Bolster and Rely on Innovations in the Information and Communications Technology Sector

As the private sector continues to innovate, federal government should look at how emerging technologies can protect our civilian networks and critical infrastructure. At a basic level, the federal government should promote the development and deployment of AI systems to monitor for network anomalies and unidentified traffic. On a deeper level, the federal government can partner with infrastructure owners and operators to promote AI usage for assessing the quality and integrity of data sets, and to monitor data flows. This added layer of protection allows AI to preemptively scan and analyze data sets to determine if they can produce negative or malicious outcomes. Additionally, AI can help monitor data traffic, determining where the data originated and its final destination. The federal government can also work with its service providers to apply these techniques to its own network systems.

2) Apply Risk-Based AI, Data Storage and Cloud-Provider Standards

Protecting data flows also means securing locations where data is stored and processed. As the federal government considers how best to secure sensitive data in the era of AI, it should consider how to verify qualified providers as well as those who will monitor the integrity of those systems. The U.S. government should partner with like-minded nations to cultivate a competitive global marketplace for trustworthy AI, data storage and cloud providers for high-risk use cases, as well as auditors and third-party verifiers, and establish governance methods to ensure trust and conformance with these frameworks. All sensitive data may not need the highest level of protection – thus, organizations should strive to further delineate sensitive data and the level of protection needed.

3) Prioritize International Interoperability

As the U.S. government seeks to formalize a governance framework for AI system and data governance, it should prioritize international interoperability. Implementing interoperable data governance standards, storage and cloud services among like-minded countries will broaden the market for trustworthy service providers, while also building more resiliency into the AI and data ecosystems.

4) Audit the Monitor

Implementing third-party verification practices and policies will be key to authenticating trust within these governance systems. Instituting protections such as zero-trust policy among data storage and monitoring vendors will add necessary security to the ecosystem, while also building and reinforcing trust.

See "Compliance Checklist for AI and Machine Learning" (Jan. 5, 2022).

5) Identify and Mitigate Risks

Congress has provided the Executive Branch with the authority to secure critical sectors of the economy. These frameworks and authorities can form the basis of a comprehensive, risk-based approach to securing AI systems and data on a sector-by-sector basis. However, a cross-sector analysis of risk should also be conducted to ensure cross-cutting risks are adequately addressed through new or existing laws and governance structures.

U.S. legislators should assess existing regulatory regimes (*e.g.*, HIPAA, Electronic Communications Privacy Act, etc.), identify gaps related to high-risk use cases, and build legislative proposals that are flexible to adapt to evolving risks. In tandem, the U.S. government should pursue public investment in trustworthy AI models and experimentation for high-risk use cases.

See Cybersecurity Law Report's two-part series on the practicalities of AI governance: "AI Governance Gets Real: Tips From a Chat Platform on Building a Program" (Feb. 1, 2023), and "AI Governance Gets Real: Core Compliance Strategies" (Feb. 8, 2023).

6) Support Public-Private Partnerships

Several principles and corresponding actions discussed in this article will rely on collaboration between government and non-government stakeholders. Many agencies within the federal government, such as NIST and the National Telecommunications and Information Administration (part of the Department of Commerce), understand how to build stakeholder coalitions to deliver actionable outcomes. Engaging industry stakeholders will be key to developing certification and monitoring activities, as well as implementing interoperable, international frameworks.

Industry and government have been working to develop partnerships and international standards to bring a deeper understanding to AI systems and data protection. Now is the time for the U.S. to lead on aligning these efforts, both domestically and internationally, into tangible governance regimes.

U.S. policymakers should continue to encourage stakeholder-driven processes to improve transparency, accountability and innovation in AI systems, including adherence to voluntary commitments, codes of conduct and risk-driven frameworks, such as the NIST AI Risk Management Framework.

Industry should define and attest to standards and codes of conduct for various categories of AI development and usage that can serve as a basis for enforcement by the FTC.

See "First Independent Certification of Responsible AI Launches" (Apr. 12, 2023).

7) Provide Targeted Safe Harbors

In implementing any comprehensive regime, compliance is key to functionality. Providing options for actors within the AI and data ecosystem (*e.g.*, apps, cloud services and data center providers) to adopt industry-certified accountability regimes will incentivize these actors to participate without fear of negative repercussions should they fall victim to malicious activity.

8) Protect Privacy and Civil Liberties

As the U.S. enters a phase of enhanced digital regulation and oversight due to increased risk from advanced technologies and a heightened threat environment, the government and organizations must ensure that governance structures and mitigation methods continue to protect and reinforce privacy and civil liberties, as well as fundamental democratic values.

9) Move Beyond Company-by-Company Bans Against High-Risk Developers

Company-by-company bans against high-risk developers are inefficient, hard to enforce and untangle, and do not adequately protect against whitelisting or restructuring. AI and data work together to maximize functionality and are in constant transformation. Thus, any regulatory framework must have the ability to mitigate existing harms while adapting to emerging threats. Static bans will never be agile enough to fully protect against risks that can emerge across the life cycle of a data-driven AI system.

See Cybersecurity Law Report's two-part series on managing legal issues arising from use of ChatGPT and Generative AI: "E.U. and U.S. Privacy Law Considerations" (Mar. 15, 2023), and "Industry Considerations and Practical Compliance Measures" (Mar. 22, 2023).

Evelyn Remaley is a partner at Wilkinson Barker Knauer, LLP, in Washington, D.C. Before joining the firm, she was Acting Assistant Secretary of Commerce for Communications and Information and Acting Administrator of the National Telecommunications and Information Administration, an Executive Branch agency, which is part of the Department of Commerce, that is principally responsible for advising the President on telecommunications and information policy issues. In that role, Remaley was also responsible for leading the Department's cybersecurity policy efforts. Prior to her federal service, she led a cybersecurity and internet policy team at Booz Allen Hamilton, where she oversaw efforts supporting a wide range of cyber policy and governance projects for the Departments of Defense and Homeland Security.