Balancing Privacy and Anti-Money Laundering Governance in the Era of Artificial Intelligence

Anna Stallings[1]

Abstract

Wide-scale deployment of Artificial Intelligence (AI) makes bold predictions about more efficient ways of detecting financial crimes, including money laundering. Contrary to the established rules-based systems checking simple transactions, AI anti-money laundering (AML) systems require more data, raising questions about privacy rights because of fragmentation in privacy laws, data hacks, compliance challenges, and unlawful activities by insiders within financial institutions. In comparison, autocracies have been prescribing data localization, dictating business practices by citing national sovereignty concerns. This research explores how adversaries could exploit privacy vulnerabilities, making this a global security challenge. Drawing on the lessons learned from the September 11 attacks and the failure of imagination, this research investigates the global security dimensions and opportunities given the diffusion of AI systems. By employing qualitative secondary analysis and causal explanation techniques, this study answers how to balance privacy rights and AML governance efficiency in the era of AI.

Keywords: Anti-Money Laundering, governance, privacy, lack of imagination, Artificial Intelligence

Equilibrio entre los derechos de privacidad y la lucha contra el lavado de dinero en la era de la inteligencia artificial

Resumen

El despliegue a gran escala de la Inteligencia Artificial (IA) hace predicciones audaces sobre formas más eficientes de detectar delitos financieros, incluido el lavado de dinero. A diferencia de los sistemas establecidos basados en reglas que verifican transacciones simples, los sistemas de IA contra el lavado de dinero requieren más datos,

1 Anna Stallings (FP8906@gmail.com)

doi: 10.18278/si.9.1.2

lo que plantea dudas sobre los derechos de privacidad debido a la fragmentación de las leyes de privacidad, los ataques de datos, los desafíos de cumplimiento y las actividades ilegales de personas internas dentro del sector financiero. instituciones. En comparación, las autocracias han estado prohibiendo la localización de datos, dictando prácticas comerciales citando preocupaciones de soberanía nacional. Esta investigación explora cómo los adversarios podrían explotar las vulnerabilidades de privacidad, lo que convierte esto en un desafío de seguridad global. Basándose en las lecciones aprendidas de los ataques del 11 de septiembre y la falta de imaginación, esta investigación investiga las dimensiones y oportunidades de seguridad global dada la difusión de los sistemas de IA. Al emplear análisis secundario cualitativo y técnicas de explicación causal, este estudio responde cómo equilibrar los derechos de privacidad y la eficiencia de la gobernanza ALD en la era de la IA.

Palabras clave: Lucha contra el blanqueo de capitales, gobernanza, privacidad, falta de imaginación, Inteligencia Artificial

在人工智能时代平衡隐私权与反洗钱

摘要

人工智能(AI)的广泛应用为关于“包括洗钱在内的金融犯罪的更有效检测方法”作出了大胆的预测。与检查简单交易的、基于规则的既定系统相反，人工智能反洗钱(AML)系统需要更多数据，进而引发了有关隐私权的问题，这归因于隐私法不完整、数据黑客、合规性挑战以及金融机构内部人员的非法活动。相比之下，独裁国家一直禁止数据本地化，以国家主权问题为由规定商业实践。本研究探究了对手如何利用隐私漏洞，使其成为全球安全挑战。基于9・11袭击和缺乏想象力所得出的教训，本研究调查了人工智能系统扩散情境下的全球安全维度与机遇。通过应用定性二次分析和因果解释方法，本研究回答了人工智能时代如何平衡隐私权与反洗钱治理效率的问题。

关键词：反洗钱，治理，隐私，缺乏想象力，人工智能

What is AML Governance?

The United States took the lead in combatting illicit financing and money laundering by implementing stricter controls on the global laundering of illegal funds. To address the growing threats related to money laundering, the Organization for Economic Co-operation and Development established the Financial Action Task Force, a group of financial experts (Abbott and Snidal 2000, 440). However, as the more recent 2022 National Strategy for Combating Terrorist and Other Illicit Financing shows, the threats continue to evolve, requiring updates to increase the detection of illicit movements. At the same time, deny illegal actors access to the U.S. financial framework (National Strategy for Combating Terrorist and Other Illicit Financing 2022, 1-4). The scale and complexity are increasing.

Divergent Views: Privacy in Democracies and Autocracies

Scholarly literature predicted how globalization and technology diffusion might spawn global change. But, as argued by Drezner (2017), states are still the driving forces in how their policy preferences are enacted in all aspects of a society under the purview of the state. Setting policies falls under the jurisdiction of the nation-state, although the approach may vary based on the government type (Drezner 2017, 477-498). In contrast to earlier times, customers now share their personal information when making ordinary purchases. Later, that email address may be sold to a data broker, often without the knowledge or recourse of a private citizen (Federal Trade Commission 2014, 1-110). This makes privacy much more critical in the era of AI.

Evidence of rising disagreement over AML governance and data is materializing amongst the nations whose values differ. For example, Google and Apple are shifting their production from China to India or Vietnam (Wakabayashi and Mickle 2022). Since the Arab Spring in 2011, in which regimes were toppled by protestors organized on common social media sites, some nations have inserted greater control over technologies (Villasenor 2011). At the center of the contention is a country like China, which views data through a national security and political lens. Inserting greater control over technologies and data in those technologies ensures data localization, meaning the data stays on the mainland (Ng 2022). This differs from the United States approach, which relies on a fragmented sectoral model for privacy rights protections. Privacy is regarded as a fundamental human right by the European Union. The collection, storage, and handling of private data are unique, as specified in the Human Rights Declaration and the European Charter of Fundamental Rights (Cunningham 2012, 651). As is shown above, privacy protections vary across the world.

As argued by Gross (2017), the right to privacy in the United States originates from a source such as the Fourth Amendment of the U.S. Constitution, which defines the right of individuals to be protected in their persons,

documents, homes, and effects against arbitrary searches and seizures. Admittedly, when the Constitution was written, technology was not as advanced, so privacy in technology was not a factor. The United States Congress approved the Electronic Communications and Privacy Act in 1986 because of technological developments. Technology has advanced, but the Act has not protected privacy rights as intended because it focuses on technology rather than public privacy concerns (Gross 2017, 73-92).

Instead, Fairclough (2016) contends that the United States depends on a fragmented sectoral model to set the guidelines for how companies collect, store, and oversee private consumer data. In that, Congress passes thoughtfully conceived statutes that do not restrain the marketplaces of self-regulation. Then, the Federal Trade Commission and the Department of Commerce monitor businesses, relying primarily on industry standards. Enterprises and firms are assumed to abide by elusive industry standards and practices they construct and interpret. Supporters of this approach argue that it helps the American business boom and that each sector knows best what works for them and their customers in today's data-driven economy (Fairclough 2016, 462-480).

Anti-Money Laundering and Privacy in the Era of Artificial Intelligence

Most Americans are familiar with HIPAA or FERPA, health privacy laws, or family education rights and privacy laws (Klosowski, 2021). However, few know that the Gramm-Leach-Bliley Act of 1999 governs how financial institutions manage customers' data (FTC 2023). These are examples of sectoral privacy rights laws of the fragmented governance approach in the United States. Others criticize this method, arguing that weaker data privacy standards mean larger profit margins (Fairclough 2016, 463-464). Despite privacy laws in place for individual states in the U.S., some states have exceptions where individuals are not notified if no financial harm is expected from the breach (Saniuk-Heinig 2021). But that raises the questions of the breached data and how illicit actors could combine it with other personal data. Recent health research also highlights the challenges associated with healthcare breaches and inadequate protection of health information. In a recent publication, Murdoch (2021) highlights the growing use of computational approaches to reidentify individuals in health data repositories. The author provides one study example, showing that an algorithm could reidentify over 80 percent of adults (Murdoch 2021, 1-5). Recent research shows how AI is making safeguarding data more difficult.

Within the AML governance, banks and financial institutions must follow several statutes to report suspicious transactions when an internal investigation makes that determination. New laws have been passed addressing money laundering, showing that this is an expanding and challenging threat to the global financial system's growing

scope and complexity. For example, in 2020, the new AML Act was passed, requiring business owners to self-disclose data, such as addresses, that will be compiled into a central registry (O'Leary 2021). Currently, the lack of prompt access to beneficial ownership information of legal entities is one limitation of U.S. AML governance. Many financial institutions have paid enormous fines for inadequate monitoring controls and missing suspicious events. For example, in 2022 alone, globally, there were $ 5 billion worth of fines (Noonan and Smith, 2023). Banks have used the rule-based system with predefined rules to monitor transactions. If there is an alert, AML professionals at the institution investigate the transaction in-depth to understand suspiciousness, which decides whether a report is filed to meet regulatory compliance.

Currently, updated capabilities such as mobile banking, widely deployed during the coronavirus pandemic, have increased overall transactions. The costs associated with monitoring and the number of false positives still need to be investigated and resolved, even if no action is taken. Overall, these tasks, when conducted manually, may be time-consuming and costly. Wide-scale deployment and diffusion of AI technology will provide institutions with a new tool that promises to work more efficiently in detecting suspicious transactions and reducing false positives. However, all this depends on how the institutions implement the AI systems. For the system to work as intended, customer features, income, geographic location, and behavioral patterns, to name a few, may have to be uploaded into AI, presenting newer privacy protection issues. Another way forward has been researched using synthetic data to train AI systems in predicting laundering (Kute et al., 2021). In the United States, the Federal Reserve describes synthetic data as generated using factual information such as social security numbers with fictional data such as the made-up birth date and name (Federal Reserve 2019).

Financial institutions paid fines for non-compliance with privacy standards outlined in internal governance models, potentially jeopardizing customer data. As an illustration, the Consumer Financial Protection Bureau (CFPB) fined one bank for illegally accessing its patron's credit reports. The staff opened checking and savings accounts, credit cards, and lines of credit, all without the customer's approval. Specifically, staff illegally retrieved sensitive personal data to apply for and open unlawful accounts (CFPB 2022). In another example, the Securities and Exchange Commission (SEC) charged Wall Street Firms with prevalent record protection violations, as the staff used personal devices to send official business communications (SEC 2022). Both examples show that sectoral self-regulation is lacking, exposing personal data to potential breaches and long-term harm to innocent consumers. In addition, today, financial institutions are the top targets for hackers (Gulyás 2023, 85). In this case, several actors could compromise personal data, or hackers could exploit a vulnerability in the system and breach the customer's data.

The recent cases show these scenarios occur more often than expected.

A Federal Trade Commission (FTC) study of 9 data brokers in the United States notes that brokers who sell data to other businesses formed sensitive extrapolations, including health-connected matters such as "diabetes interest," ethnicity, income levels, and wealth. In addition, American people technically do not "own" their personal information, so there is no way even to fix mistaken data (FTC 2014, 1-110). Privacy does not address the most up-to-date technologies, such as online tracking behavior through web browsers and the increase of the marketplace for personal data, including the third parties' relationships and the sharing of data (GAO-13-663 2013).

As argued by Milaj and Kaiser (2017) and financial data supplies very nuanced customer information, including familial and individual habits. Transaction monitoring should be made rationally when deciding how much personal, sensitive data will be integrated into AI systems. The decision should consider the inherent fragmentation of the governance in privacy protections and detecting suspicious activities. Even if one were to look at the European Union (EU) AML governance which has been heralded as the privacy data standard setter, data transaction retention is also at the point of contention for individual rights to privacy and data safeguards. The enormous amount of data in transaction history supplies an incredibly detailed look at a person's life and habits, mainly if unsuspicious transactions are kept. In the EU, financial institutions must store the transactions for five years after the business relationship with the customer. The transaction history holds data about the customer's employment, earnings, benefits, housing payments, and grocery shopping. Specific personal details, such as health or political beliefs, may be inferred from a person's transaction record, making it highly sensitive. This information may contradict privacy laws. For example, there may be monthly charges from a political party or contributions to a religious association (Milaj and Kaiser 2017, 115-125).

Global Security Dimensions

Given the fragmented sectoral approach to privacy rights, it is essential to clearly say why privacy-related challenges would be considered a global security challenge. To answer this question, one only needs to return to the lessons learned from the commission reports following the September 11th terrorist attacks. The report sheds light on how analytical failure of imagination limited understanding of terrorists and their methods. Clarke (2010), in his book Cyberwar, argues that in the proceeding days before the invasion of Iraq, psychological operations wre used right before the onset of combat operations. Although willing to engage in a psychological campaign before the war, Clarke (2010) notes that the administration was reluctant to disrupt Iraqi financial assets. The attorneys feared that draining financial institutions would be seen by other countries

as a breach of international principles. The United States decided against pursuing this course of action, but the discussion alone shows the significance of the financial systems with war (Clarke 2010, 9).

These examples show how fragmented privacy protections in the era of AI could be exploited in a future military scenario if the data were compromised. AI technology is much more efficient in creating targeted disinformation or propaganda that could be made from stolen, leaked, or hacked financial data to target American soldiers during the initial stages of a crisis, with specific messages when they would be most needed to prepare for war. As laid out in the *Handbook of Propaganda*, psychological operations targeting military members are nothing new, as history is replete with examples going back decades (Colley 2020). In contrast, AI technology enables the production and delivery of very targeted psychological operations that could include data from breached or stolen data. As Bateman (2020) emphasizes, AI's fast improvement has opened the door for the fabrication of deceptive, deepfake videos and convincing fake photos and writing. When employed customized, these approaches can be wielded as disinformation tools, resulting in varying levels of harm to targeted individuals (Bateman 2020). Notably, an authoritarian regime that does not always recognize international law may be more willing to use data this way as part of targeted psychological operations campaigns and disinformation against American troops as part of psychological warfare before a potential onset of conflict. That brings me to the second part of the global security dimensions. One finding of the 9/11 Commission Report cites a lack of imagination and a way of thinking that disregarded possibilities as one aspect of not supplying indications and warnings on suicide pilots before the attack. This was in the backdrop of the 1995 Manila air plot to crash an explosives-laden plane into government headquarters (9/11 Commission Report 2004, 336).

In addition, as an example, one of China's Three Warfare strategies is psychological warfare. It aims to weaken potential enemies in combat by discouraging, dissuading, and shocking their armed military members and supportive populations (Iasiello 2016, 51). A scenario involving an adversary of America exploiting fragmented privacy protections in a potential military conflict, using advanced technologies like AI for psychological operations to gain an advantage on the battlefield, is plausible.

Opportunities

The Federal Trade Commission could strengthen its monitoring capabilities by clearly defining its legal principles under Section Five of the Federal Trade Commission Act. Over time, the Federal Trade Commission could notify companies and specify a pattern leading to increased enforcement (Fairclough 2016, 474). Standards for managing private data and legislative and administration considerations for adopting AI systems in financial

institutions' AML governance should be adapted. As AI technology diffuses, ethics about how AI alerts a transaction for potential laundering should be considered (Kute 2021). Artificial Intelligence AML systems could use generative models to develop the ability to establish genuine but synthetic clients with no relationship to real people, like using AI in medicine without inputting patient data into larger systems (Murdoch 2021, 5).

Some states have already begun taking some measures, and others should follow. The California Consumer Protection Act (CCPA) provides patrons the right to demand that a commercial company remove any personal information about the consumer that the enterprise collected with laid-out privacy notices (The California Protection Act 2019). The CCPA also supplies the right to ask data brokers to disclose to the customers what data they have gathered, how it has been used, and to whom it has been sold or with whom it has been shared (U.S. Data Product Privacy Notice 2023).

Based on the recent trends, it is likely that financial institutions will remain top cyber security targets. The information technology staff at institutions should apply vigorous adaptive protection methods that search for and reduce unseen cyber exploits. After a breach, an essential step for security administrators is to find the foundational aspects of a breach. Using forensics to examine traffic should be urgent in deciding the basis of the violation. Trained staff should focus on data capture, studying all traffic for irregularities and signs of problems in the network, and charting results of exploration and system weaknesses for review (Opara 2017, 138-160).

Conclusion

Artificial Intelligence makes manipulating breached, leaked, stolen or bought private financial data in the opportune moments to create sophisticated disinformation or psychological operations targeting the American people during a crisis seem plausible. Artificial Intelligence allows for more effective use of technology, including potential use in psychological operations. It should be imagined that one of America's adversaries could employ this tactic in a potential conflict. Taking preventive measures such as establishing clear guidelines that limit the exposure of private information in the AI AML systems should be a priority before financial institutions deploy this technology more broadly.

Anna Stallings is a doctoral student in Global Security and holds an MA in Security Studies and an MS in Strategic Intelligence. She welcomes opportunities for continued research and collaboration.

Bibliography

Abbott W. Kenneth and Snidal Duncan. 2000. "Hard and Soft Law in International Governance." *International Organization*, Summer, 2000, Vol. 54, No. 3, Legalization and World Politics (Summer, 2000), pp. 421-456.

U.S. Data Product Privacy Notice 2023. Acxiom. https://www.acxiom.com/privacy/us/consumer-instructions/.

Bateman, Jon. 2020. "Deep fakes and Synthetic Media in the Financial System: Assessing Threat Scenarios." *Carnegie Endowment for International Peace.*

California Consumer Privacy Act of 2019. https://oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf

CFPB Fines U.S. Bank $37.5 Million for Illegally Exploiting Personal Data to Open Sham Accounts for Unsuspecting Customers. 2022.

Clarke, Richard A. (Richard Alan), and Robert K. Knake. 2010. *Cyber War: The Next Threat to National Security and What to Do about It*. 1st ed. New York: Ecco.

Cunningham, McKay. 2012. "Privacy in the Age of the Hacker: Balancing Global Privacy and Data Security Law Privacy." *The George Washington International Law Review* 44 (4): 643-695. http://ezproxy.apus.edu/login?

Drezner, W. Daniel. The Global Governance of the Internet: Bringing the State Back In. *Political Science Quarterly.* Vol. 119, No. 3 (Fall, 2004).

Fairclough, Bradyn. 2016. "Privacy Piracy: The Shortcomings of the United States' Data Privacy Regime and How to Fix." *Journal of Corporation Law* 42 (2): 461–80.

Federal Trade Commission (FTC). 2014. "Data Brokers A Call for Transparency and Accountability." https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf (Accessed 2 January 2024).

Federal Trade Commission. 2023. Federal Trade Commission | Protecting America's Consumers (ftc.gov) (Accessed 2 January 2024).

Federal Reserve. 2019. The Federal Reserve System White Paper Examines the Effects of Synthetic Identity Payments Fraud. Federal Reserve Board - Federal Reserve System white paper examines the effects of synthetic identity payment fraud.

GAO-13-663. 2013. "Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace." https://www.gao.gov/products/gao-13-663. (Accessed 2 January 2024).

Gross, Shannon. 2017. "A Mystery Wrapped in an Encryption: Surveillance and Privacy in the Encrypted Era." *Northwestern Journal of Technology and Intellectual Property* 15 (1): 73-92. http://ezproxy.apus.edu/login?

Gulyás, Olivér, and Gábor Kiss. 2023. "Impact of Cyber-Attacks on the Financial Institutions." *Procedia Computer Science* 219: 84–90. https://doi.org/10.1016/j.procs.2023.01.267.

Iasiello, Emilio. 2016. "China's Three Warfare Strategy Mitigates Fallout from Cyber Espionage Activities." *Journal of Strategic Security.* Volume 9, Number 2, 2016.

Klosowski, Thorin. 2021. "The State of Consumer Data Privacy Laws in the U.S. and Why it Matters." 2021. *New York Times*. The State of Consumer Data Privacy Laws in the U.S. (And Why It Matters).

Kute, Dattatray Vishnu, Biswajeet Pradhan, Nagesh Shukla, and Abdullah Alamri. 2021. "Deep Learning and Explainable Artificial Intelligence Techniques Applied for Detecting Money Laundering-A Critical Review." *IEEE Access* 9: 82300–317. https://doi.org/10.1109/ACCESS.2021.3086230.

Milaj, Jonida, and Carolin Kaiser. 2017. "Retention of Data in the New Anti-Money Laundering Directive 'Need to Know' versus 'Nice to Know.'" *International Data Privacy Law* 7 (2): 115–25. https://doi.org/10.1093/idpl/ipx002.

Murdoch, Blake. 2021. Privacy and Artificial Intelligence: Challenges for Protecting Health Information in a New Era. 2021. *BMC Medical Ethics.* 2021. 22:122. https://doi.org/10.1186/s12910-021-00687-3.

National Strategy for Combating Terrorist and Other Illicit Financing. 2022. National Strategy for Combating Terrorist and Other Illicit Financing (treasury.gov). (Accessed 1 January 2024).

Ng, Wendy. 2022. "The Role of Competition Law in Regulating Data in China's Digital Economy." *The Chicago Law Journal.* 84 (3): 841-81.

Noonan Laura and Smith Allen. 2023. Global Anti Money Laundering Fines Surge by 50 %. Global anti-money laundering fines surge at 50% | Financial Times (ft.com)

O'Leary, Brendan. 2021. "The Corporate Transparency Act: A Step Toward Broken Shells." *Journal of Legislation* 47 (2): 133.

"Strategic Narratives and War Propaganda." 2020. *The SAGE Handbook of Propaganda*. https://search.credoreference.com/articles/Qm9va0FydGljbGU6NTA4NzU=. (Accessed 1 January, 2024).

Opara, Emmanuel U., and Mohammed T. Hussein. 2017. "Cyber Security, Threat Intelligence: Defending the Digital Platform." *Journal of International Technology & Information Management* 26 (1): 138–60. doi:10.58729/1941-6679.1287.

Rojas L, Alonso E, Axelson S (2012). "Money Laundering Detection Using Synthetic Data." In: The 27th annual Swedish Artificial Intelligence Society (SAIS) Workshop, Karlskrona.

Saniuk-Heinig, Cheryl. 2021. State Data Breach Notification Chart. https://iapp.org/resources/article/state-data-breach-notification-chart/ . (Accessed 1 January, 2024).

SEC Charges 16 Wall Street Firms with Widespread Recordkeeping Failures, Firms Admit to Wrongdoing and Agree to Pay Penalties totaling More than $1.1 Billion. 2022. SEC.gov | SEC Charges 16 Wall Street Firms with Widespread Recordkeeping Failures

The 9/11 Commission Report. 2004. The 9/11 Commission Report (9-11commission.gov)

Wakabayashi, Daisuke and Tripp Mickle. 2022. "Tech Companies Slowly Shift Production Away from China." *The New York Times*, September 6. http://ezproxy.apus.edu/login?

Villasenor, John. 2011. Recording Everything: Digital Storage as an Enabler of Authoritarian Governments. *Center for Technology Innovation at Brookings.*