

Privacy Regulation Roundup – April 2024

This Privacy Regulation Roundup summarizes the latest major global privacy regulatory developments, announcements, and changes. This report is updated on a monthly basis. For each relevant regulatory activity, you can find actionable Info-Tech analyst insights and links to useful Info-Tech research that can assist you with becoming compliant.

Contents

[Can Generative AI be Both Powerful and Private? 3](#_Toc163042670)

[**Type:** News](#_Toc163042671)

[**Announced:** March 2024](#_Toc163042672)

[TikTok Faces Uncertain Future: US House Passes Divestiture Bill Amid Security Concerns Error! Bookmark not defined.](#_Toc163042673)

[**Type:** Legislation](#_Toc163042674)

[**Announced:** March 2024](#_Toc163042675)

[UN adopts US-led resolution on AI development 5](#_Toc163042676)

[**Type:** Announcement](#_Toc163042677)

[**Announced:** March 2024](#_Toc163042678)

[Navigating the Data Seas: Unpacking China’s New Cross-Border Data Transfer Regulations Error! Bookmark not defined.](#_Toc163042679)

[**Type:** Regulation](#_Toc163042680)

[**Announced:** April 2024](#_Toc163042681)

[The MGM CyberAttack: Lessons Learned 6](#_Toc163042682)

[**Type:** News](#_Toc163042683)

[**Announced:** April 2024](#_Toc163042684)

`

# Can Generative AI Be Both Powerful and Private?

**Type:** News

**Announced:** March 2024

**Summary:** I've seen tech privacy problems for around three decades, and in my opinion, these AI chatbots are the next wave. They're attractive to use – they'll make work easier – but we need to keep our eyes on how they handle personal information. Companies gather data and boom, suddenly it's out there, even stuff people never meant to share. These AI companies train their systems on everything – your emails, medical searches, the works. Then someone hacks them, or the system generates private stuff by mistake. Lawsuits are already starting, regulators are looking hard, but the laws are weak. We need to fix that, or this AI privacy mess is just the beginning.

The scary part is that this isn't just Big Brother collecting your info. AI systems can analyze your info and guess stuff about you that was never even written down. Suddenly, they have this digital clone that sounds just like you. Privacy is about more than someone stealing your credit card – it's about your whole identity being up for grabs. I'm not saying AI is evil, but we need safeguards in place that will reduce our vulnerability. It's a tough balance, and right now, the law on this is a mess. We need rules that protect us, not just a series of loopholes for companies to slip through.

**Analyst Perspective:** Generative AI's immense potential is shadowed by growing privacy concerns. While these tools can streamline tasks and unlock insights, their reliance on vast amounts of data raises red flags. Personal information, often gathered without consent, faces potential disclosure or misuse. The ability of generative AI to infer deeply personal details poses a unique risk, going beyond traditional data brokering practices, and could lead to highly accurate digital impersonations that pose security and reputational threats.

Existing privacy laws weren't designed for this scale of data use, leaving gaps in protection. Companies need to be transparent about their models' training and respect user choices. Lawmakers need to act quickly, or the archives of our digital lives will become raw material for a new kind of privacy intrusion, leaving us with little control over how our personal information is used and likely exploited.

**Analyst:** [Carlos Rivera](https://www.infotech.com/profiles/carlos-rivera), Principal Advisory Director – Security & Privacy

**More Reading:**

* Source Material: [IAPP](https://iapp.org/news/a/large-language-models-present/), [AXIOS](https://www.axios.com/2024/03/14/generative-ai-privacy-problem-chatgpt-openai)
* Related Info-Tech Research:
  + [*Conduct an AI Privacy Risk Assessment*](https://www.infotech.com/research/ss/conduct-an-ai-privacy-risk-assessment)
  + [*Address Security and Privacy Risks for Generative AI*](https://www.infotech.com/research/ss/address-security-and-privacy-risks-for-generative-ai)
  + [*Build Your Generative AI Roadmap*](https://www.infotech.com/research/ss/build-your-generative-ai-roadmap)

**TikTok Faces Uncertain Future: US House Passes Divestiture Bill Amid Security Concerns**

## Type: Legislature

## Announcement Date: March, 2024

**Summary**: In a significant bipartisan decision, the US House of Representatives has approved a bill aimed at TikTok, the popular video-sharing platform. The legislation, which saw a resounding victory with 352 votes in favor and 65 against, requires TikTok to disentangle itself from its Chinese parent company, ByteDance, or risk a nationwide prohibition. This swift legislative move is a response to long-standing concerns about national security risks associated with ByteDance’s potential access to data from American users. Despite TikTok’s assurances about data privacy and the absence of evidence indicating data misuse, lawmakers have been prompted to act. This action was influenced by recent classified briefings and the app’s perceived influence on US politics. The passage of the bill in the House signifies a growing agreement on the need to tackle the issues presented by apps owned by foreign entities. However, it is subject to constitutional examination due to potential violations of free expression rights and the singling out of a specific company operating in the US. As the bill progresses to the Senate, it receives support but also encounters obstacles, including doubts about its legal solidity and the implications for free speech and privacy. The Senate’s decision remains uncertain, as the bill needs thorough examination to resist potential legal objections.

**Analyst Perspective**: The US House of Representatives’ recent legislative action against TikTok, a popular video-sharing platform owned by China’s ByteDance, carries significant implications. The potential for a more secure digital environment in the US could increase user trust in domestic platforms. However, the move may heighten US-China tensions in the digital realm and raise global digital governance norms questions. The situation underscores the scrutiny foreign-owned apps face and the importance of data privacy in international relations. It also highlights the challenges multinational digital platforms face navigating complex regulatory environments. In essence, the TikTok situation is a critical point in the technology, policy, and international relations intersection, emphasizing the complexities businesses face in today’s interconnected digital world.

**Analyst**:[Horia Rosian](https://www.infotech.com/profiles/horia-rosian), Director – Cybersecurity & Privacy, Workshops

**More Reading:**

* Source Material: [House passes bill that could ban TikTok in the U.S., sends to Senate - The Washington Post](https://www.washingtonpost.com/technology/2024/03/13/tiktok-ban-passes-house-vote/)
* Related Info-Tech Research:
  + [*Build a Data Privacy Program*](https://www.infotech.com/research/ss/build-a-data-privacy-program)
  + [*Mature Your Privacy Operations*](https://www.infotech.com/research/ss/mature-your-privacy-operations)
  + *Build a Security Compliance Program*

# UN Adopts US-Led Resolution on AI Development

**Type:** Announcement

**Announced:** March 2024

**Summary:** The UN General Assembly (UNGA) announced the adoption of a US-led draft resolution on the adoption of artificial intelligence. Described as a “landmark” document by the UNGA, the resolution:

* Situates respect and protection of human rights and freedoms as the compass that should guide AI development at all stages of the lifecycle of AI systems.
* Recognizes the potential of AI systems to significantly enable and accelerate progress toward desirable goals such as the UN’s [Sustainable Development Goals](https://www.un.org/sustainabledevelopment/sustainable-development-goals/), promoting digital transformation, overcoming digital divides between countries, and more.
* Warns against the many potentially adverse impacts of AI systems developed without adequate safeguards and attention to human rights, including hindering progress toward the goals mentioned, undermining information integrity, and interfering with personal privacy.

Additionally, the document encourages all member states to:

* Promote safe, secure, and trustworthy artificial intelligence systems in an inclusive and equitable manner.
* Develop domestic regulatory approaches to support responsible and inclusive AI innovation.
* Develop safeguards for individual privacy and the protection of personal data.
* Bridge digital divides between and within countries.
* Ensure disability, gender, and racial equality perspectives are always included in policy decisions.

The scope of AI systems in this resolution was limited to those in the non-military domain and was adopted without a vote.

**Analyst Perspective:** This wide-ranging resolution is notable as the UN’s first resolution intended to guide the development of AI systems. It is also notable that it was adopted without a vote, which in the context of the UNGA, signals that there was no opposition from any of the member countries. There are similarities between the language in this resolution and previous statements from the US government, notably [Executive Order 14110](https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence).

The resolution does not require any member state or the UNGA itself to take concrete action. Instead, it is a basis for future action: a set of guiding principles and a vision that governments, international agencies, regulatory bodies, and civil actors may adapt or adopt as their own. Ensure you establish your own guiding principles for AI use and development that considers the demands of your customers, partners, regulators, and legislation, and establish governance that can ensure those principles are embedded in organizational practices.

**Analyst:** [Andrew Sharp](https://www.infotech.com/profiles/andrew-sharp), Research Director – Infrastructure & Operations

**More Reading:**

* Source Material: [UN News](https://news.un.org/en/story/2024/03/1147831)
* Related Info-Tech Research:
  + [*Develop Responsible AI Guiding Principles*](https://www.infotech.com/research/ss/develop-responsible-ai-guiding-principles)
  + [*Govern the Use of AI Responsibly With a Fit-for-Purpose Structure*](https://www.infotech.com/research/ss/govern-the-use-of-ai-responsibly-with-a-fit-for-purpose-structure)
  + [*Conduct an AI Privacy Risk Assessment*](https://www.infotech.com/research/ss/conduct-an-ai-privacy-risk-assessment)

# Navigating the Data Seas: Unpacking China’s New Cross-Border Data Transfer Regulations

## Type: News

## Announcement Date: April, 2024

**Summary**: In the rapidly evolving digital landscape, China has recently introduced significant changes to its cross-border data transfer (CBDT) laws. These changes mark a shift from the previously stringent controls to more relaxed measures, aimed at facilitating international business and fostering growth in the digital economy. One of the key highlights of the new regulations is the introduction of exemptions for certain types of data transfers. Specifically, data transfers related to international trade and emergencies are now exempt from the previous CBDT legal mechanisms. This change is expected to streamline operations for businesses involved in these areas. Furthermore, the new regulations have raised the thresholds for triggering CBDT legal mechanisms. This is particularly beneficial for businesses handling non-sensitive personal information, as it eases their compliance burden. However, despite these relaxations, businesses must not overlook the importance of compliance. The article emphasizes the need for thorough data mapping and strict adherence to Chinese laws. It also underscores the importance of staying updated with sector-specific guidelines. Although the new CBDT regulations in China offer more flexibility for businesses, they also necessitate a strategic approach to data management. As such, multinational corporations operating in China must stay abreast of these changes and adjust their data management practices accordingly. This will not only ensure compliance but also help them leverage the opportunities presented by China’s burgeoning digital economy.

**Analyst Perspective**: The recent modifications to China’s cross-border data transfer (CBDT) laws present a mixed bag of opportunities and challenges for multinational corporations. The eased measures and exemptions could potentially simplify operations and reduce compliance-related costs, making China a more appealing market for international businesses, particularly in the digital sector. However, the complexity of the regulatory environment persists. Ensuring compliance will require businesses to maintain robust data management practices and stay abreast of sector-specific guidelines, which could involve significant investments of time and resources. These changes underscore the strategic importance of data management. Businesses that can effectively navigate these regulatory shifts may gain a competitive edge in China’s rapidly growing digital economy. Despite the increased flexibility, the new CBDT regulations highlight the need for businesses to remain agile and informed amidst evolving data governance landscapes. This is especially relevant in today’s data-driven global economy, where effective data management can be a key differentiator.

**Analyst**:[Horia Rosian](https://www.infotech.com/profiles/horia-rosian), Director – Cybersecurity & Privacy, Workshops

**More Reading:**

* Source Material: [China's new cross-border data transfer regulations: What you need to know and do (iapp.org)](https://iapp.org/news/a/chinas-new-cross-border-data-transfer-regulations-what-you-need-to-know-and-do/)
* Related Info-Tech Research:
  + [*Build a Data Privacy Program*](https://www.infotech.com/research/ss/build-a-data-privacy-program)
  + [*Mature Your Privacy Operations*](https://www.infotech.com/research/ss/mature-your-privacy-operations)
  + *Build a Security Compliance Program*

# The MGM Cyberattack: Lessons Learned

**Type:** News

**Announced:** April 2024

**Summary:** On the evening of Friday 8th September 2023, MGM Resorts in Las Vegas experienced a cyberattack that began with a phone call to the company's tech support. The caller, posing as an employee, claimed to have forgotten their password. The organization subsequently realized that this was a hacker gaining unauthorized access to MGM's systems. Over the following five days, this group, known as Star Fraud, attempted to extort over $30 million from MGM.

Star Fraud emerged from the online community known as the Com, a network of cybercriminals primarily driven by status and money rather than a passion for technology. Exploiting a weakness in tech support systems, the hacker group infiltrated MGM's corporate networks, prompting the company to shut down some systems, including email, to thwart the attack. Despite MGM's efforts, the attack disrupted operations and drew global attention, with long lines forming at hotel front desks and casino floors thrown into manual operation mode. Star Fraud demanded a ransom to decrypt MGM's systems, which the company refused to pay.

The attack cost MGM approximately $100 million in lost revenue and incurred expenses of approximately $10 million for cybersecurity response efforts. While the hackers managed to access customer names and contact information, MGM asserts that credit card and bank information remained secure. The FBI advises against paying such ransoms, but many victims still opt to do so, highlighting the ongoing threat posed by cybercriminals to businesses worldwide.

**Analyst Perspective:** The attack highlights the importance for organizations to have a robust [privacy program](https://www.infotech.com/research/ss/build-a-data-privacy-program) and to be prepared to respond to ransomware threats. Businesses need to prioritize data privacy and security as part of their overall risk management strategy. This includes implementing measures to protect sensitive customer information, such as personal details and financial data, from unauthorized access.

Having a well-defined incident response plan in place is crucial for swiftly addressing cyberattacks. The plan should outline procedures for detecting, containing, and mitigating the impact of security incidents, including ransomware attacks among others. Additionally, regularly backing up data and maintaining offline backups can help businesses recover quickly in the event of a ransomware attack. This ensures that critical systems and information can be restored without paying ransom demands.

Collaborating with industry experts, threat intelligence service providers, and law enforcement agencies can provide valuable insights and support in responding to cyber threats and attacks. More importantly, employees should be trained to recognize social engineering tactics used by hackers, such as impersonation, phishing emails, and pretexting. Vigilance and skepticism can help prevent unauthorized access to systems and data.

MGM demonstrated a strong stance against cyber extortion and a willingness to invest in long-term security measures. Refusal to pay the ransom reflects its resilience and commitment to protecting its data and operations, despite falling victim to a cyberattack – ultimately reinforcing its reputation as a responsible organization.

**Analyst:** [Safayat Moahamad](https://www.infotech.com/profiles/safayat-moahamad), Research Director – Security & Privacy

**More Reading:**

* Source Material: [IAPP](https://iapp.org/news/a/ransomware-group-requested-30m-from-las-vegas-casino-during-data-breach/), [The Wall Street Journal](https://www.wsj.com/tech/cybersecurity/mgm-hack-casino-hackers-group-0366c641)
* Related Info-Tech Research:
  + [*Build Resilience Against Ransomware Attacks*](https://www.infotech.com/research/ss/build-resilience-against-ransomware-attacks)
  + [[*Develop and Implement a Security Incident Management Program*](https://www.infotech.com/research/ss/develop-and-implement-a-security-incident-management-program)](https://www.infotech.com/research/ss/govern-the-use-of-ai-responsibly-with-a-fit-for-purpose-structure)