Robinson+Cole

CYBERSECURITY

CISOs: New Report Outlines Risks of LLMs

I hang out with a lot of Chief Information Security Officers (CISOs), so this piece is for them. Of course, it will be of interest to all security professionals struggling with assessing the risk of large language models (LLMs).

According to DarkReading, Berryville Institute of Machine Learning (BIML) recently issued a report entitled "An Architectural Risk Analysis of Large Language Models: Applied Machine Learning Security," which is designed "to provide CISOs and other security practitioners with a way of thinking about the risks posed by machine learning and artificial intelligence (AI) models, especially LLMs and the next-generation large multimodal models so they can identify those risks in their own applications."*Read more*

DATA PRIVACY

California Privacy Protection Agency Launches New Website with Privacy Rights Resources

Last week, California Attorney General Rob Bonta announced a new enforcement focus on streaming apps' failure to comply with the California Consumer Privacy Act (CCPA). This investigation will examine whether streaming services are complying with the opt-out requirements for businesses that sell or share consumers' personal information as required by the CCPA. Specifically, the agency will examine those services that do not offer an easy mechanism for consumers to exercise this opt-out right. *Read more*

DATA SECURITY

Mercedes-Benz Source Code Potentially Compromised in GitHub Token Exposure

Mercedes-Benz reportedly suffered a security incident that exposed confidential source code on an Enterprise Git server. The incident occurred due to a compromised GitHub exposed by an employee. Although the incident occurred on September 29, 2023, it wasn't discovered until January 11, 2024. A cybersecurity firm discovered the token during an internet scan and informed Mercedes-Benz, which quickly revoked it. *Read more*

ARTIFICIAL INTELLIGENCE

Italian Data Protection Authority Alleges Breaches of GDPR by ChatGPT Platform

On January 29, 2024, the Italian Data Protection Authority (Garante) notified OpenAI of breaches of data protection laws involving its ChatGPT platform. *Read more*

February 1, 2024

FEATURED AUTHORS:

Linn F. Freedman
Kathryn M. Rattigan
Blair V. Robinson

FEATURED TOPICS:

Artificial Intelligence
Cybersecurity
Data Privacy
Data Security
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C Website
LinkedIn
Twitter
Facebook

PRIVACY TIP #387

AI and Deepfakes: What to Know and How to Spot Them

Spotting deepfakes is like spotting a phishing email. Most people think they can spot them, but is that really the case? As deepfakes and AI-generated content quality will improve and get harder to detect, it's important to educate yourself on ways to determine when something is real or is deepfaked. Find out more in today's Privacy Tip.
Read more

RECENT EVENTS AND NEWS

Artificial Intelligence Team lawyer Sean Griffin will be among the speakers presenting at the New England Claim Executives Association February 2024 Meeting. Sean's presentation, entitled "AI and Claims Handling," will cover the impact artificial intelligence (AI) has on claims, a history of where it started, the future of AI in claims, the current pitfalls and upside, and the concern that AI may replace adjusters. For more information, click here.

ABOUT ROBINSON+COLE

Robinson+Cole is an AmLaw 200 law firm established over 179 years ago, with a deeply-rooted culture of collaboration, civility, and inclusion. The Mansfield Rule Certified Plus-firm has more than 250 lawyers in eleven offices throughout the Northeast, Mid-Atlantic, Florida, and California, serving regional, national, and international clients, from start-ups to Fortune 50 companies. For more information, please visit www.rc.com.

Boston | Hartford | New York | Washington, DC | Providence | Miami
Stamford | Wilmington | Philadelphia | Los Angeles | Albany | **rc.com**