MEALEY'S® LITIGATION REPORT

Artificial Intelligence

Generative AI, Cybersecurity And Cybercrime For Lawyers: Myths, Risks And Benefits

By
Dr. Ilia Kolochenko

Platt Law LLP
New York, NY

and

Michael P. Heiskell

National Association Of Criminal Defense Lawyers
Fort Worth, TX

A commentary article reprinted from the June 2024 issue of Mealey's Litigation Report: Artificial Intelligence

LexisNexis®

Commentary

Generative AI, Cybersecurity And Cybercrime For Lawyers: Myths, Risks And Benefits

By
Dr. Ilia Kolochenko
and
Michael P. Heiskell

[Editor's Note: Dr. Ilia Kolochenko is a Partner and Cybersecurity Practice Lead at Platt Law LLP. Being a cybersecurity expert, he has over 15 years of professional experience in information security auditing and cybercrime investigations. Dr. Ilia Kolochenko is also an Adjunct Professor of Cybersecurity & Cyber Law at Capitol Technology University, and a CLE Faculty Member at the DC Bar teaching cybersecurity course there. Michael Heiskell is the current President of the National Association Of Criminal Defense Lawyers. He is also a former state and federal prosecutor and whose current practice focuses on White Collar criminal defense and investigations. He is also a former President of the Texas Criminal Defense Lawyers Association and a member of its Hall of Fame. Heiskell is a forthcoming inductee into the American College of Trial Lawyers at its Annual Meeting in Nashville in September 2024. Any commentary or opinions do not reflect the opinions of Platt Law LLP, the National Association of Criminal Defense Lawyers or LexisNexis®, Mealey Publications™. Copyright © 2024 by Dr. Ilia Kolochenko and Michael P. Heiskell. Responses are welcome.]

I. Brief history of Artificial Intelligence

Many legal professionals have probably first heard of the allegedly omniscient AI chatbots – powered by Generative AI (GenAI) based on mysterious Large Language Models (LLMs) – in late 2022, when OpenAI pompously announced its first public release of the ChatGPT chatbot. However, early prototypes of GenAI, as well as human-like chatbots, have their roots in the mid-sixties with ELIZA, one of the first chatbots made available for public in 1966 by Joseph Weizenbaum at MIT.[1] Historically, the mathematical genesis and some scientific foundations of modern GenAI can be traced back to 1906 with the invention of Markov-chain models.[2] Notwithstanding the remarkably long history of GenAI, during the twentieth century, its development was comparatively modest and slow, marked with several systemic disappointments and disillusionments relating to its practicality, operability or economic viability compared to other technologies.

However, about a decade ago, industry interest in AI regained momentum, namely due to the rapid technological progress and wide availability of powerful and cost-efficient hardware. Siri, the emblematic digital assistant from Apple, pioneered the contemporary use of more powerful AI chatbots with its integration into Apple's iOS in 2011. Importantly, the truly groundbreaking discovery for modern LLM-powered GenAI happened in 2017, when researchers from Google proposed a new deep-learning AI architecture called transformer,[3] taking GenAI to the next level of performance and machine intelligence. Since then, the speed of AI development, fueled by unprecedented attention from Big Tech and concomitant multi-billion investments, started its exponential growth around the globe. To illustrate the pace and scale of modern-day AI progress, one may look at a public repository of AI models, maintained by a well-known AI startup Hugging Face, that hosts over 600,000 AI models as of May 2024.[4]

Unsurprisingly, the highspeed AI race propels fears and uncertainty in society. Legal professionals are

no exception, having reasonable worries about job security, unwarranted and unfair monopolization of human knowledge by Big Tech, malicious use of AI by hostile nation states and organized crime, and the overall future of humanity. In addition, criminal defense attorneys are concerned about the use and impact of AI in the area of law enforcement by virtue of predictive policing, face recognition and profiling, that may infringe both constitutional and statutory privacy rights, being susceptible to inaccuracy and bias. Today, certain AI vendors claim that their LLMs – trained predominantly on data with origins that are kept strictly confidential – are as intelligent as most human beings or even smarter. To reassure readers, it is worthwhile noting that many emerging AI vendors exaggerate the miraculous or magic-like capabilities of their arcane AI technology,[5] to put it mildly. Paradigmatically, some GenAI startups – formerly figuring among the most promising and successful investments of prominent VC funds – are starting to face overwhelming financial challenges,[6] triggered by, among other things, non-viable economic models, tough competition and investors who become gradually more prudent and even skeptical when dealing with AI promises. This is not to mention a formidable tsunami of lawsuits against big and small GenAI vendors, and emerging AI legislation on both sides of the Atlantic.[7] Ironically, the only certain winner in the AI startups race is Anguilla, a British Overseas Territory in the Caribbean, that administers its national ".ai" top-level domain (TLD). In 2023, the $32 million dollar revenue from the ".ai" domain sales represented more than 10% of Anguilla's GDP.[8]

II. Yet another failed attempt to declare extinction of the legal profession

Nostalgically, some legal professionals still recall the golden epoch of the late nineties marked with the global excitement and enthusiasm about the Internet. Some naïve futurists truly believed that the Internet would make legal profession redundant and obsolete, eventually leaving most lawyers unemployed. Their premature forecasts and underpinning arguments were bolstered with the launch of Internet search engines, where one could easily find a contract template virtually for any matter or even obtain "legal advice" on a modestly designed website or in a nascent generation of Internet chats and forums. That being said, the Internet, as well as ubiquitous digitalization, have materially reshaped virtually every single dimension of the legal profession. However, the digital revolution, also skyrocketed the volume of international trade and inevitable disputes, increasing the demand for lawyers more than ever. The pervasive digitalization, simultaneously improved and accelerated numerous routine tasks and time-consuming legal processes. Illustratively, today, it would be almost impossible to find a lawyer who would prefer undertaking case law research digging through dusty books in a law library instead of using his or her computer, especially when clients are becoming increasingly more gourmand in relation to speed and cost-efficiency of lawyering. The simple aftermath of the Internet revolution is that twenty years later we still have lawyers and the Internet, co-existing in a synergizing harmony.

The second *déjà-vu* episode of the emotionally heralded saga predicting the extinction of lawyers, emerged several years ago with the invention of smart contracts, which were designed to eliminate most bankers and legal professionals. The road to hell is paved with good intentions: some people unfortunately believed such promises, mostly promulgated by selfish vendors and startups offering all kind of products and services relating to smart contracts, without making much research on the subject matter. Although, the notorious Credit Suisse and Silicon Valley Bank debacles shook the global banking industry, the collapses are highly unlikely be attributed to the invention of smart contracts that, on their side, sunk into oblivion with some narrow exceptions. Nevertheless, the underlying blockchain technology will undoubtedly remain useful for divergent business tasks in banking and financial industries, enhancing reliability, security and efficiency of the global financial system.

Analogously, Machine Learning and Artificial Intelligence, including the now-overhyped GenAI, will certainly make a significant change in the legal profession, improving and accelerating many trivial but laborious tasks and processes, as will be briefly discussed below. The change will, however, be far away from a tectonic or revolutionary nature, as some commentators promise. Moreover, the change will unlikely happen within one or even two years, rather gradually taking place during the next decade. Importantly, GenAI will probably once again create an impetus for global trade and economy, and again make lawyers more demanded than ever. Thus, another major attempt to declare extinction of the legal profession has failed.

III. Security, privacy and legal risks of GenAI for lawyers

Unbeknownst to some legal practitioners, Machine Learning and AI, including pre-LLM architectures of GenAI, have been broadly and successfully used in the legal profession for over a decade already. Triage and classification of e-discovery data, digital platforms for legal research and case law analysis, contract editing and review software – are just a few examples of AI-powered tools utilized by lawyers and legal professionals on a daily basis. Next generation of AI tools offer even more powerful capabilities for lawyers, such as, the prediction of most successful arguments or motions before a specific judge or court based on the precedents. While their operational value is obvious, they also carry out significant security, privacy and legal risks that the reader should be aware of.

First, whenever submitting any internal documents – being it a client memo, newly drafted M&A agreement, or governmental subpoena just-received by a corporate client – to any third-party systems, ensure that there is a crystal-clear understanding how this data will be utilized. The unequivocal warning made by the FTC in February 2024, proactively reminding tech companies that a stealth update of their terms of service to exploit customer data for AI training purposes could be unfair and deceptive,[9] remained largely unheeded especially among smaller vendors and startups. If a proprietary or client-related data ends up in an AI training dataset, chances that an LLM, subsequently trained on the data, discloses small excerpts or even large chunks of the documents are pretty high. Moreover, some creative manipulations and command prompt engineering with LLMs may allow attackers to gradually extract portions of the underlying training data for further misuse. Therefore, ensure that any and all documents that are sent to a cloud, third-party managed or operated storage, are duly protected from unauthorized use.

Second, those law firms that contemplate building their own AI systems on internally available data, should consider nominating a Data Protection Officer (DPO). Several years ago, the DPO role was mostly focused on personal data protection within a company. Nowadays, the role has been expanded to cover a broad spectrum of legal issues stemming from GenAI, for instance, the use of copyrighted, privileged or confidential data for AI training purposes, in addition to the use of personal data in AI training datasets. A DPO should also build and continually maintain a comprehensive organizational data flow chart, comprehensively depicting internal and external data flows of the organization, paying special attention to AI-related data flows. Whenever data is utilized for AI training purposes, the underlying technical and legal risks should be thoroughly and regularly assessed. For instance, Article 53 of the newly enacted EU AI Act, expressly requires covered entities to have a company-wide policy to prevent copyright infringement. While most US law firms will unlikely be covered by the EU AI Act and its provisions, they should, nonetheless, be prepared to comply with the ballooning number of privacy laws on both state and federal level, as well as with novel data protection rules and privacy regulations by administrative agencies. Most of the recently enacted privacy laws grant individuals a diversified pallet of privacy rights, spanning from the right to be informed how their personal data is used to the right to correct or even delete their personal data. Exercise of those rights are commonly embodied in Data Subject Requests (DSR), when an individual may request a law firm or any other data controller – within the timeline provided by applicable law – to erase his or her personal data. This task can be just technically impossible with certain architectures of AI models: as recently admitted by OpenAI and then aptly used by famous Max Schrems's European Center for Digital Rights project (also known as "noyb") to lodge a complaint against OpenAI with the Austrian DPA, which may ultimately lead to a gigantic monetary fine against OpenAI and even possible ban of ChatGPT in the EU member states.[10] To avoid similar hurdles, add data privacy by design and by default principles to all AI projects and initiatives.

Third, whenever using GenAI to draft any kind of legal or client-related documents, ensure that the final content is always manually reviewed by a lawyer. The problems of the so-called hallucinations will unlikely be resolved in the near future, opening a floodgate of inaccurate and erroneous content synthesized by bizarre AI deviations. The rapidly increasing number of anecdotical cases, when lawyers carelessly file lawsuits or motions with non-existent case law or fake statutory provisions, may appear amusing at first sight. Courts are, however, pretty far from sharing such a charitably cheerful view on the negligent use of GenAI by lawyers,[11] readily suspending careless member

of the profession for up to one year in addition to other legal ramifications.[12] Moreover, sophisticated cyber-attacks against AI vendors and their supply chains are poised to balloon. For instance, poisoning of training data can be exploited for country-wide disinformation campaigns or creation of purposely harmful content, spanning from backdoored software to dangerous medical advice.[13] Thus, establish a holistic and regularly reviewed AI policy at the law firm that would define, govern and operationalize permissible use of AI with specific and effective guardrails.

IV. Cybercrime and cybersecurity trends in 2024 for lawyers

Most legal professionals have already been victims of innumerable forms and harsh consequences of cybercrime. Some had their social media accounts stolen and exploited for blackmailing, others faced costly ransomware attacks at their law firms, entailing devastating financial, legal and reputational consequences. This is not to mention recent, nation-wide attacks on Critical National Infrastructure (CNI) objects, leaving entire cities without access to healthcare, electricity, water or gas. Other attacks paralyzed schools, governmental agencies and even law enforcement units[14] and police officers in charge of investigating cybercrime.[15] While some cyber threat actors are motivated exclusively by profits and purposely attack the most vulnerable and most susceptible to pay ransom, others are primarily driven by ideology, furthering their political views amid the unfolding geopolitical crisis. This is not to mention elite teams of hackers backed by foreign nation states actively engaged in cyber war, which is now shifting from the Internet to space, targeting satellites and other orbital technologies.[16]

The current climate of uncertainty, fear and doubt relating to cybercrime is unfortunately further propelled by some cybersecurity and fraud prevention vendors imprudently making speculative claims about multi-trillion-dollar losses caused by cybercrime. According to the FBI's Internet Crime Complaint Center (IC3) report, US entities and individuals lost over $12.5 billion dollars in 2023 due to cyber-attacks, representing a grim 22% year-over-year growth.[17] It should be noted, however, the prudent numbers provided by the FBI include only reported or disclosed cybersecurity incidents and intrusions, which represent just a tip of the immense cybercrime iceberg. The truth lays somewhere in between: direct financial losses mostly converge towards the prudent FBI numbers. Oppositely, more subtle and nuanced indirect losses – that require a significant effort to be precisely measured – such as reputational impact and eventual loss of profits, let alone the decade-long effect of trade secret theft, may indeed hit a trillion dollars in a multi-year perspective.

Despite the soaring intensity and amplitude of cyber-attacks, the technical complexity of underlying hacking techniques does not always follow the evolution.[18] At first sight, it may appear counterintuitive and even illogical, however, there is a sound explanation of the trend. Contrasted to most lawful sectors of the economy, contemporary cybercrime is a mature, well-organized and hierarchically disciplined, highly efficient and effective industry with enormous potential for relentless growth. Modern-day cybercriminals are unemotionally pragmatic and are good at math: they always search the easiest, least costly, and most riskless ways to steal information or compromise systems to eventually demand ransom. For instance, instead of attacking a leading financial institution – that can afford to invest tens of millions in its cybersecurity program and to hire best-of-breed cybersecurity professionals – astute cybercriminals will rather stealthily compromise one of the financial institution's trusted third parties that either have full copies or a privileged access to exactly the same data. Third parties usually include external accountants, financial auditors, law firms, IT and even cybersecurity vendors, and all other kinds of external firms and professionals. Resultingly, hacked law firms – including some of the largest ones – make news headlines in media with an unenviable frequency.[19] Addressing the issue of hardly detectable but extremely dangerous supply chain attacks, organizations are rushing to implement Third-Party Risk Management (TPRM) programs, while lawmakers and regulators include TPRM requirements into data protection laws and regulations.

The problem is, however, much broader than just countless third and fourth parties having access to corporate crown jewels. The working from home (WFH) trend, ubiquitous mobile and connected devices, chaotic migration to multi-cloud environments, ad hoc deployment of new software and hardware solutions to keep pace with technical progress – dramatically increase the external attack surface of organizations, as well as the number of trivially exploitable weak-

nesses and vulnerabilities. Tellingly, over 80% of cloud data breaches are actually caused by human misconfigurations of otherwise perfectly securable cloud infrastructure.[20] Organizations rush to migrate their data to the cloud, hoping to save their costs and improve performance, but forget to accommodate and train their software developers, IT managers and even cybersecurity personnel accordingly. Resultingly, even the most secure cloud-based products become a treasure trove even for beginner cybercriminals, who can simply download gigabytes of most sensitive corporate data in plaintext from a misconfigured and publicly exposed cloud storage. Therefore, with some narrow exceptions, most organizations including law firms, can be compromised without possessing extraordinary hacking skills in 2024.

V. GenAI and its impact on cybercrime

With publicly accessible GenAI bots and other online tools, made freely available by deep-pocketed tech giants or generously VC-backed AI startups in lavish marketing efforts to advertise their ostensibly magical AI products, the novel technology undoubtedly plays a tangible role in the proliferation of cybercrime. Yet, despite the unstoppable supply of scaremongering reports and press releases describing omnipotent capabilities of GenAI and their catastrophic impact on cybercrime surge, most of the underlying claims are either over-dramatized or just technically incorrect. Having said this, a justified rationale for anxiety about the emerging technical capabilities of GenAI and their fermenting effects on cybercrime does exists.

The new generation of LLM-powered GenAI provides dangerously potent capacity to generate top-quality deep fakes, including photos, audio and video recordings that, inter alia, that can be exploited to bypass biometric authentication systems. Formerly, before the wide-scale operationalization of LLMs with billions of parameters, the earlier forms of GenAI could produce the very same type of fake content, however, its quality was poor and would unlikely fool even a child, let alone forensic experts. Contrastingly, modern GenAI has become a Swiss army knife for cybercriminals and online fraudsters, which can be utilized to write impeccably looking phishing emails or to create fake but credibly looking web pages and PDF documents. Those nefarious generative capabilities can be perfidiously exploited to impersonate government and law enforcement agencies, big and small corporations, banks and insurances, law firms or even individuals to empty their bank accounts by fooling a bank hotline.[21] Given that, according to the 2024 Data Breach Investigations Report (DBIR) by Verizon, human error figures among the primary causes of intrusions and data breaches,[22] one should not downplay the impact of emerging capacities and capabilities of GenAI-equipped cyber intruders. To make things even worse, quite some AI vendors – trying to impress each other or their now-enthusiastic investors – provide uncontrolled access to their GenAI tools for free, while putting from little to no guardrails to prevent malicious use of their technology.

Distilling the foregoing, it is important to say that deceptive capabilities of organized cybercrime have been sufficiently advanced and inventive to successfully manipulate their victims during past decade. Years before the launch of ChatGPT, well-organized gangs of cyber mercenaries already had access to professional copywriters, psychologists and even lawyers to create top-quality content, obviously concealing their real identities and the contemplated use of deliverables from the unwitting professionals. Paradigmatically, apart from creation of deceptive content, aiming at perfidiously misleading human beings, GenAI remains comparatively useless for skilled cybercriminals. For example, GenAI cannot deploy compromised infrastructure as a proxy to conceal real sources of cyber-attacks, GenAI cannot launder and cash out ransomware proceeds received in crypto currencies, and GenAI cannot verify that new "clients" of cyber gangs are not undercover agents of the FBI or the DOJ. Finally, GenAI's malware creation capabilities remain quite primitive and nascent, bringing from little to no value for experienced cybercrime groups.[23] In a nutshell, while cybercrime is booming for a variety of interconnected reasons briefly discussed above, GenAI is not, and will unlikely become, a groundbreaking or revolutionary facilitator of data breaches in 2024.

VI. Benefits of GenAI for the legal profession

Nowadays, even the most developed countries including the US and UK offer a suboptimal access to justice, especially for people from socially vulnerable groups, racial or ethnic minorities.[24] Sluggish, expensive and operationally inefficient legal and judicial systems lead to, among other things, wrongful convictions and miscarriage of justice.[25] In addition, coer-

cive guilty plea tactics and the trial penalty employed by some prosecutors, and too often sanctioned by the courts, contribute as well to these egregious results. For instance, public defenders for indigent defendants in criminal cases are so overloaded with snowballing cases, that sometimes have to spend less than an hour per case that would normally require at least several full days of a thorough preparation.[26]

Sadly, even a well-prepared trial by top-ranked lawyers from a Big Law global firm, is no guarantee of acquittal for an innocent person. Most state and federal courts experience relentlessly increasing backlogs due to the mounting number of cases, often the result of overcriminalization. Eventually, judicial system – including prosecutors and judges – foreseeably handles and closes avalanching cases in an expeditious manner, without having a luxury to examine every detail of a case, inevitably hurting both the quality and fairness of the due process. This socially dangerous phenomenon is, however, not a creature of the American legal system as one may think. For example, even traditionally calm and untroubled Switzerland faces identical challenges.[27]

In response to the foregoing challenges, GenAI can be the next evolutionary, but not revolutionary, step of continuous improvement of the legal profession. Properly implemented GenAI systems can swiftly clean up judicial bottlenecks and streamline litigation without impacting its quality, impartiality or fairness. For instance, equipped with a pretty simple GenAI tool, a lawyer can get a one-page summary of a case, encompassing the most relevant, decisive and otherwise legally important elements of the dossier, assembled and summarized from hundreds of various court documents, search warrants, handwritten notes, forensic investigation reports, depositions and photographs. Moreover, AI can occasionally be even more attentive and accurate than a legal professional on a late Friday evening after a busy day in court.

The automation will, however, not replace lawyers in other crucial tasks that truly deserve and require human skills, reasoning and knowledge. Likewise, in its current state, GenAI cannot depose a witness or convince the jury, but can save a considerable amount of valuable human time in preparation of these processes. Importantly, as briefly discussed above, while AI can greatly assist summarizing and prioritizing human-readable content, a lawyer should always carefully review the documents and scrutinize all AI-generated creations, otherwise, an innocent person may end up behind the bars because of a single AI hallucination. Similarly, court clerks and judges can leverage the speed of GenAI to accelerate and streamline their caseload, putting the most important dossiers and urgent motions on top of the decreasing pile of cases, quickly getting to the most decisive elements of a case, precisely spotted and cogently summarized by AI. Prosecutors, on their side, can utilize AI to predict chances that an accused will be convicted, based on the previously available data, avoiding wasting their limited time on tempting but hopeless cases. However, many dangerous collateral effects of AI could develop in criminal justice system. For example, prosecutors can mechanically utilize AI to mathematically predict chances that an accused will be convicted in a jury trial – based just on the previously available statistical data – and vigorously press charges. That inherent danger potentially removes human consideration of the many mitigating, and often exculpatory, evidence and subtle circumstances that weigh against a prosecution from the onset. So, in considering this burgeoning field of GenAI and its impact on criminal justice system, one must be vigilant in identifying biases this emerging technology may often create and foster. It is essential to implement creative safeguards to ensure the presumption of innocence is maintained as the overriding principle in court system.

VII. Conclusion

This article attempted to demystify and debunk some popular myths about cybersecurity, cybercrime and AI by separating the wheat from the chaff, in parallel offering a concise factual overview of the current state of Artificial Intelligence in the legal profession.

Combination of the speed of AI with unique cognition, perception and reasoning of human brain can make access to justice more open and efficient, prevent discrimination and injustice, and considerably improve the current state of legal practice, making it both less stressful for legal professionals and more affordable, effective and beneficial for clients.

In sum, the future of the legal profession belongs, as always, to lawyers, who will be progressively assisted

by various digital tools and solutions including those ones powered by GenAI.

Endnotes

1. Al-Amin, M., Ali, M.S., Salam, A., Khan, A., Ali, A., Ullah, A., Alam, M.N. and Chowdhury, S.K. (2024) "History of generative Artificial Intelligence (AI) chatbots: past, present, and future development", arXiv preprint arXiv:2402.05122.

2. Lencastre, P., Gjersdal, M., Gorjão, L.R., Yazidi, A. and Lind, P.G. (2023) "Modern AI versus century-old mathematical models: How far can we go with generative adversarial networks to reproduce stochastic processes?", Physica D: Nonlinear Phenomena, 453, p.133831.

3. Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A.N., Kaiser, Ł. and Polosukhin, I. (2017) "Attention is all you need", Advances in neural information processing systems, 30

4. Hugging Face, "Models", accessible at: https://huggingface.co/models

5. Bort, J. (2023) "I'm an AI software engineer and I predict that most AI startups being funded today will die", Business Insider, July 14, accessible at: https://www.businessinsider.com/ai-engineer-explains-why-most-ai-startups-will-die-2023-7

6. Mann, T. (2024), "Stability AI reportedly ran out of cash to pay its bills for rented cloudy GPUs", The Register, April 3, accessible at: https://www.theregister.com/2024/04/03/stability_ai_bills/

7. Kolochenko I. (2024), "GenAI: Copyright and Beyond", New York Law Journal, March 28, accessible at: https://www.law.com/newyorklawjournal/2024/03/28/genai-copyright-and-beyond/

8. Bubola E. (2024), "The A.I. Boom Makes Millions for an Unlikely Industry Player: Anguilla", New York Times, March 23, accessible at: https://www.nytimes.com/2024/03/22/business/artificial-intelligence-anguilla.html

9. Federal Trade Commission (2024), "AI (and other) Companies: Quietly Changing Your Terms of Service Could Be Unfair or Deceptive", February 13, accessible at: https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/02/ai-other-companies-quietly-changing-your-terms-service-could-be-unfair-or-deceptive

10. NOYB - European Center for Digital Rights (2024), "ChatGPT provides false information about people, and OpenAI can't correct it", April 29, accessible at: https://noyb.eu/en/chatgpt-provides-false-information-about-people-and-openai-cant-correct-it

11. Olson K. (2024), "Judge sanctions attorney misled by AI, offers 'broader lesson' to bar", Massachusetts Lawyers Weekly, February 22, accessible at: https://masslawyersweekly.com/2024/02/22/judge-sanctions-attorney-misled-by-ai-offers-broader-lesson-to-bar/

12. Warwick B. (2024), "Colorado lawyer suspended for using AI platform to draft legal motion", CBS News, November 22, accessible at: https://www.cbsnews.com/colorado/news/colorado-lawyer-artificial-intelligence-suspension/

13. Kolochenko I. and Platt G. (2023), "Data Security, Professional Perspective - ChatGPT: IP, Cybersecurity & Other Legal Risks of Generative AI", Bloomberg Law, accessible at: https://www.bloomberglaw.com/external/document/X7K3GI38000000/data-security-professional-perspective-chatgpt-ip-cybersecurity-

14. SWI (2023), "Hackers steal Swiss police and customs data", June 3, accessible at: https://www.swissinfo.ch/eng/politics/hackers-steal-swiss-police-and-customs-data/48563830

15. BBC (2023), "Greater Manchester Police officers' details hacked in cyber attack", September 14, accessible at: https://www.bbc.com/news/uk-england-manchester-66810756

16. Tepper E. (2022), "The First Space-Cyber War and the Need for New Regimes and Policies", CIGI Policy Brief, No. 173

17. FBI Internet Crime Complaint Center (2024), "FBI Internet Crime Report 2023", accessible at: https://www.ic3.gov/media/pdf/annualreport/2023_ic3report.pdf

18. ImmuniWeb (2023), "Top 5 Cybersecurity and Cybercrime Predictions for 2024", accessible at:

https://www.immuniweb.com/blog/top-5-cybersecurity-and-cybercrime-predictions-for-2024.html

19. Skolnik S., Witley S. and Cohen O. (2023), "Law Firm Cyberattacks Grow, Putting Operations in Legal Peril", Bloomberg Law, July 7, accessible on: https://news.bloomberglaw.com/business-and-practice/law-firm-cyberattacks-grow-putting-operations-in-legal-peril

20. Chaudhary A. (2023) "Managing Cloud Misconfigurations Risks", Cloud Security Alliance (CSA), August 14, accessible at: https://cloudsecurityalliance.org/blog/2023/08/14/managing-cloud-misconfigurations-risks

21. Purdy K. (2024), "Fake AI law firms are sending fake DMCA threats to generate fake SEO gains", Ars Technica, April 4, accessible at: https://arstechnica.com/gadgets/2024/04/fake-ai-law-firms-are-sending-fake-dmca-threats-to-generate-fake-seo-gains/

22. Verizon Inc. (2024), "2024 Data Breach Investigations Report (DBIR)", accessible at: https://www.verizon.com/business/resources/reports/dbir/2024/summary-of-findings/

23. Scroxton A. (2024), "AI will heighten global ransomware threat, says NCSC", Computer Weekly, January 24, accessible at: https://www.computerweekly.com/news/366567396/AI-will-heighten-global-ransomware-threat-says-NCSC

24. Rapping J. (2012), "Redefining Success as a Public Defender: A Rallying Cry for Those Most Committed to Gideon's Promise", NACDL's The Champion®, Issue June 2012, Page 30

25. Oppel R. and Patel J. (2019), "One Lawyer, 194 Felony Cases, and No Time", New York Times, January 31, accessible at: https://www.nytimes.com/interactive/2019/01/31/us/public-defender-case-loads.html

26. Nicholas M. Pace, Malia N. Brink, Cynthia G. Lee and Stephen F. Hanlon (2023), "National Public Defense Workload Study", July 27, accessible here: https://www.rand.org/pubs/research_reports/RRA2559-1.html

27. Di Stephano L. (2024), "Olivier Jornot: «Sans renforts, il sera difficile de tenir la baraque»", April 30, accessible at: https://www.tdg.ch/justice-genevoise-le-nombre-de-procedures-explose-305587216168 ■

MEALEY'S LITIGATION REPORT: ARTIFICIAL INTELLIGENCE
edited by Bryan Redding
The Report is produced monthly by

LexisNexis®

1600 John F. Kennedy Blvd., Suite 1655, Philadelphia, PA 19103, USA
Telephone: (215)564-1788 1-800-MEALEYS (1-800-632-5397)
Email: mealeyinfo@lexisnexis.com
Web site: http://www.lexisnexis.com/mealeys
ISSN 2994-1105