

Modern Lawyer

Ideas for Legal Leaders

Editor: Alex Davies

July 2026 www.globelawandbusiness.com

Featured in this issue

Managing cyber security risk as a law firm

Can we prompt privacy?
Navigating vendor AI without breaching client duties

Protection of client data in the era of AI

A large illustration of an iceberg floating in a blue ocean under a blue sky with white clouds. The iceberg's tip is visible above the water, while its much larger, jagged base is submerged below the surface. A horizontal bar with a multi-colored pixelated pattern separates the top text area from the main image.

**Cyber risks –
beware the
hidden dangers**



It's an uncomfortable truth that cybercrime is becoming more of a "when" than an "if" scenario – especially with AI getting in on the act and working furiously around the clock to exploit systems. What's perhaps even more concerning are the hidden dangers that are happening, essentially legally.

This issue of *Modern Lawyer* looks at data protection in the legal profession from a range of different angles, reaching a common conclusion – that law firms can no longer treat cyber security and AI governance as optional, and that the greatest threats are perhaps

less obvious than we imagine.

On p11, Dr Ilia Kolochenko argues that the greatest emerging threat comes from the growing ecosystem of AI tools that lawyers use every day. He warns that confidential client information may be inadvertently shared with AI vendors through default settings, cloud-based services, mobile devices and connected technologies. He makes the argument that firms must actively manage data flows, minimize unnecessary data storage, review privacy settings and adopt robust governance measures if they are to protect client confidentiality in the AI era.

On p57, Jelena Schidzig takes a more conceptual and provocative approach, arguing that the legal profession is focusing on the wrong risk. While AI vendors often reassure users that they do not train models on uploaded documents, she contends that the real value lies in the metadata surrounding legal work – patterns of activity, workflows and the development of legal reasoning. Existing confidentiality rules, contracts and compliance frameworks are primarily designed to protect documents and their contents, not the behavioral and structural information that AI systems can learn from. Jelena argues that protecting client interests in the future will require a new approach centered on governance of legal data infrastructure rather than simply controlling access to documents.

Finally, on p35, Matt Reed focuses on the practical realities of cyber security risk management for law firms, particularly small and medium-sized practices with limited budgets and expertise. He argues that because law firms hold highly sensitive personal and commercial information, leadership teams must take responsibility for understanding and managing cyber risk. Firms need to identify their biggest vulnerabilities, test their resilience to incidents such as ransomware attacks, scrutinize suppliers, adopt recognized security standards and develop a culture of ongoing risk reduction. His message is that proactive investment in cyber security is now a fundamental business requirement and far less costly than responding to a major breach.

Cyber security clearly remains a major concern – and perhaps not always in the way we might expect.

Alex Davies

Editor

Editor

Alex Davies

Editorial board

Ida Abbott

Jeremy Barton

James Collis

Neville Eisenberg

Heidi Gardner

Tony King

Moray McLaren

Charles Martin

Stephen Mayson

Rebecca Normand-Hochman

Aline Poncelet

Kenny Robertson

Bjarne Tellmann

Globe Law and Business contacts

Sian O'Neill, Managing Director

sian@globelawandbusiness.com

Nicola Hornsby, Marketing Manager

nicola@globelawandbusiness.com

To contribute

The Editor and Globe Law and Business welcome new contributions.

Proposals for new articles/
material should be submitted to
Alex Davies at

Alex@globelawandbusiness.com

Citation

This journal should be cited as
MLP Vol 10 [2026]

To subscribe contact

glo@globelawandbusiness.com

Annual subscription

Digital £375/\$595/€485

Contact

glo@globelawandbusiness.com
for multi-user options

Modern Lawyer is published by

Globe Law and Business Ltd

3 Mylor Close, Horsell, Woking

Surrey GU21 4DD

Tel: +44 20 3745 4770

The idea for this journal arose from the 'Business of Law' series of books, which is co-published with the International Bar Association. The journal is complementary to the book series, and the publishers gratefully acknowledge the support of the IBA.

Contents

Volume 10, Issue 2, July 2026

2

Considering a career change? – why CILEX CPQ is a good route

By Phil Manning

5

Neurodiversity in law – moving from adjustment to advantage

By Pam Loch

11

Protection of client data in the era of AI

By Dr Ilia Kolochenko

15

Top tips for corporate counsel

By Dr Thomas Loest

23

“What are *you* doing here?” How lawyers can maintain credibility when it is challenged

By Susan Heaton-Wright

27

How corporate law departments can use process and technology to lose friends and alienate people

By Nate Cemenska

32

When it comes to AI, HR must set the example

By Rachel Street

35

Managing cyber security risk as a law firm

By Matt Reed

39

The rise of the portfolio career

By Layla El-Wafi

44

All change? Mental health in the legal sector

By Kim Tasso

51

From firm strategy to team reality – why alignment keeps failing in law firms

By Bill Cooper

57

Can we prompt privacy? Navigating vendor AI without breaching client duties

By Jelena Schidzig

66

Building a sustainable culture of business development in law firms – a three-pronged approach

By David Freeman

70

Why Gallup's State of the Workplace Report is concerning reading for legal leaders

By Rob Cross

Protection of client data in the era of AI

By Dr Ilia Kolochenko



Lawyers and law firms of all sizes have been targeted by both cyber mercenaries and nation-state hackers for over a decade.¹ The former are mainly motivated by greed and purposely look for easy targets – more than a few law firms are understandably inclined to silently pay a ransom to get their stolen data back and to avoid devastating publicity. The latter are instead going after the confidential data of wealthy or influential clients, whose personal and professional secrets may be a matter of national security, or even reveal information that could weaken global dominance in a specific industry.

With the proliferation of AI-powered tools, solutions, and online services in our daily lives, the cybersecurity threat landscape is evolving rapidly, creating unprecedented risks and challenges for the legal industry. Among the less obvious cybersecurity trends, propelled by AI, is the fact that the cyber risk created by nefarious cybercriminals is progressively overshadowed by the risk emanating from legitimate AI vendors, ranging from AI powerhouses to tiny AI start-ups.

Some AI vendors receive privileged and highly confidential client data directly from negligent law firms, many of which are motivated to share their crown jewels without due precaution by the fear of missing out on the now-fading AI hype.² Other AI enterprises invent creative and often dubious tactics to stealthily obtain valuable data from unwitting lawyers and law firms, which AI vendors so desperately need to train their data-hungry models. This article briefly discusses the new classes of cyber risks to be considered and mitigated by lawyers and other legal professionals, including ADR professionals.³

The first and the most prominent risk does not stem from the use of AI-powered legal-tech tools specifically designed for legal practice, but rather from traditional and ancillary software used by lawyers on a daily basis. In 2026, it would be an arduous task to find a single online conferencing solution, email, or other office tool, or client relationship management software that has not yet released a set of AI-enabled features and capabilities, trying to impress each other with pompous press releases.

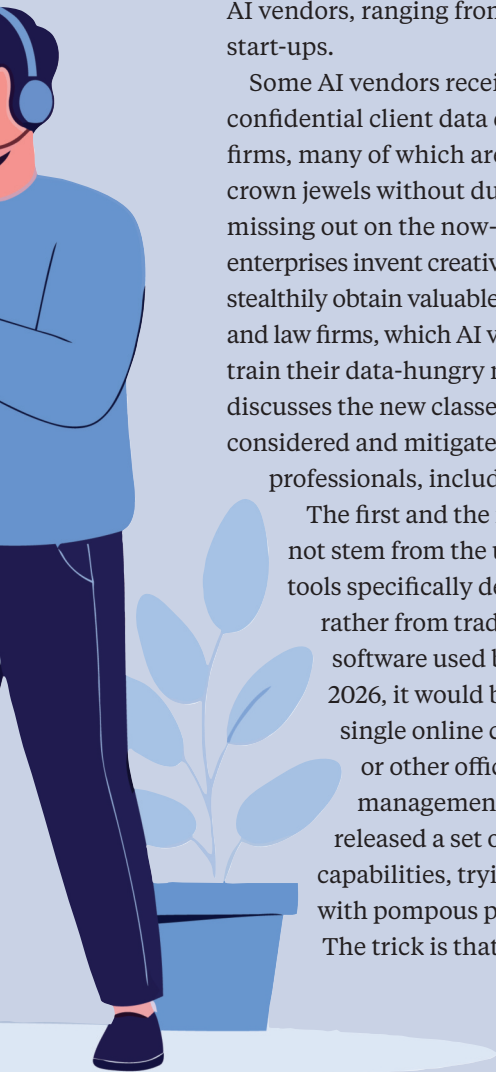
The trick is that many such tools enable

With the proliferation of AI-powered tools, solutions, and online services in our daily lives, the cybersecurity threat landscape is evolving rapidly, creating unprecedented risks and challenges for the legal industry.

data-sharing for AI training purposes by default, be it legal or otherwise in many jurisdictions. It means that all you say or all you type may be quietly sent to external software companies under the convenient pretext of continuous improvement of solutions or under the guise of better user experience. Disabling such default configuration may be time-consuming and counterintuitive.

Regrettably, the use of so-called Dark Patterns, aimed at subconsciously manipulating and preventing users from disabling data sharing, has become a prevalent practice in the modern IT industry. Therefore, it is good practice to check the security and privacy settings of your Microsoft, Adobe, or Zoom products – to name just a few – to verify what is being shared and for what purposes. The same applies to all kind of online platforms and apps that lawyers use for both personal and professional needs. For instance, reviewing the privacy settings of your LinkedIn or WhatsApp accounts is a sound way to begin compiling the inventory of messages, posts, conversations, and other fruit of your intellectual labor and daily work that might end up being used for AI training purposes unbeknownst to you. This is not to mention the worst-case scenarios of data leakage discussed below.

The second risk stems from the wide range of both freely and commercially available AI chatbots and similar online services promising some sort of magic. Although corporate subscriptions from the giants of the AI industry tend to provide decent data protection on paper, it may be technically impossible to comply with these terms of service or even with a custom and hard-negotiated data



Lawyers who undertake confidential calls with a client, judge, or prosecutor commonly forget that everything they say may be automatically recorded by their smart home devices and then sent to a foreign cloud.

protection agreement. For instance, with the surge of cyber-attacks against AI chatbots, all AI vendors protect their large language models (LLM) via multilayered cyber-defense.

In practice, this means that all the queries, documents, or scans sent to a cloud-based AI chatbot will go through a list of third-party cybersecurity solutions to ensure that input is not malicious. The question is whether you know who these cybersecurity vendors are and what they actually do with your data. Data protection agreements with AI vendors rarely provide a lot of details on these technical but essential matters, usually briefly saying something about data-sharing with third parties to the extent provided or permitted by law. While defending their own intellectual property and preventing data breaches is the inalienable right and even duty of AI

companies, this should not be done at the expense of your clients' confidentiality. Of note, even large AI vendors are embroiled in questionable data-sharing practices,⁴ evidencing that even a multi-billion-dollar valuation tag on an AI vendor is not a quality seal of transparent and ethical data use practices.

Needless to say that when you upload your legal brief, expert witness report, or M&A contract to be checked by a freely available chatbot, it is likely that all the content will be permanently kept and later exploited for AI training and other, even less obvious, but riskier, purposes. To make things worse, smaller AI vendors actively create so-called data-sharing pools. By continually submitting their (your) training data to the pool, participants become eligible to receive some or even all data from the pool submitted by other participants. In that case, once your most sensitive data ends up in such a pool, it will be dispersed across the internet without the technical possibility to ever delete it or even to find traces of who has access to it.

The third risk derives from the mixture of AI with the Internet of Things (IoT), smart objects, and mobile devices. In recent years, all sorts of gadgets have become omnipresent in our homes, streets, and offices.⁵ The problem is that most of the wearable and other objects send your personal and other data to a cloud for storage and processing. Being a treasure trove for AI vendors, your personal data from IoT and other smart devices is frequently shared or sold to them with a tiny notice buried somewhere in the middle of an IoT manufacturer's privacy policy.

This extract from the article 'Protection of client data in the era of AI' by Dr Ilia Kolochenko, is from the July 2026 edition of *Modern Lawyer*, published by Globe Law and Business.

To subscribe go to: www.globelawandbusiness.com/journals/Modern-Lawyer-Journal

Two ways to subscribe to *Modern Lawyer*:

1. Subscribe today and receive a 15% discount, go to:

<https://www.globelawandbusiness.com/journals/Modern-Lawyer-Journal>

2. Email '*Modern Lawyer* subscriber offers' to

jenny@globelawandbusiness.com

What's included in **Modern Lawyer Plus?**



Modern Lawyer

© 2026 Globe Law and Business Ltd (Except where otherwise stated) All rights reserved. No part of this publication may be reproduced in any material form (including photocopying, storing in any medium by electronic means or transmitting) without the written permission of the copyright owner, except in accordance with the provisions of the Copyright, Designs and Patents Act 1988 or under terms of a licence issued by the Copyright Licensing Agency Ltd, 6-10 Kirby Street, London EC1N 8TS, United Kingdom (www.cla.co.uk, email: licence@cla.co.uk). Applications for the copyright owner's written permission to reproduce any part of this publication should be addressed to the publisher.

DISCLAIMER

This publication is intended as a general guide only. The information and opinions which it contains are not intended to be a comprehensive study, nor to provide legal advice, and should not be treated as a substitute for legal advice concerning particular situations. Legal advice should always be sought before taking any action based on the information provided. The publishers bear no responsibility for any errors or omissions contained herein.

ISSN 2634-548X



9 772634 548005 >