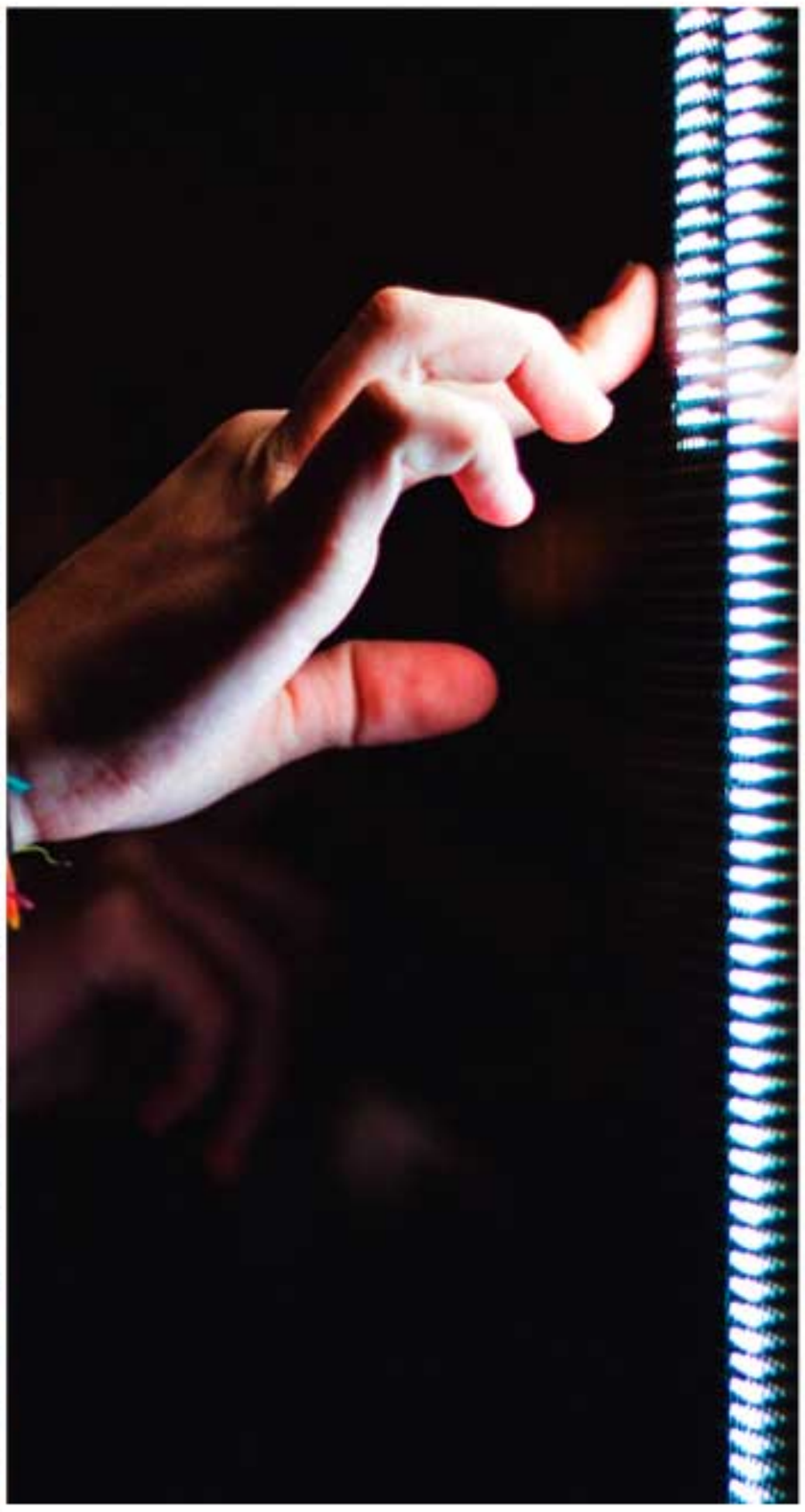


LE & TRAN
TRIAL LAWYERS

LE & TRAN
LAW CORPORATION

NEWS SPOTLIGHT

Don't type your secrets into ChatGPT

Source: Business Times (Apr 2023)

Stephen Le
www.letranlaw.com

LE & TRAN
TRIAL LAWYERS

LE & TRAN
LAW CORPORATION

Does it ever feel like you're "talking" to Google or ChatGPT?

The disarming use of our everyday language leads many of us to treat these tools as though they were a magic mirror connected only to our keyboard.

Stephen Le
www.letranlaw.com

Swipe for more / 02

LE & TRAN
LAW CORPORATION

It's easy to forget that both Google and ChatGPT are connected to enormous databases, run by complex algorithms and employ deep data analytics. The average user likely would not consider that real people will almost certainly see whatever is typed into those harmless-looking search bars.

Stephen Le
www.letranlaw.com

LE & TRAN
LAW CORPORATION

South Korean technology giant Samsung painfully re-learned this lesson recently.

According to reports, three of the company's information technology staff thought it was a good idea to enter confidential information into ChatGPT.

One employee asked the chatbot to check sensitive source code for errors, another asked it to help optimise a string of crucial hardware code, and a third fed it a recorded team meeting and asked it to generate minutes.

Stephen Le
www.letranlaw.com

Swipe for more / 04

LE & TRAN
LAW CORPORATION

There's nothing Samsung can do about it

Presumably, the three developers were under pressure and moving too quickly. That's the most likely cause of the blunder. But it's also possible they considered their session with the chatbot to be secure.

Whatever the motive behind the mistake, it no longer really matters because OpenAI (ChatGPT's parent company) effectively now has access to some of Samsung's trade secrets, and there's nothing Samsung can do about it.

Stephen Le
www.letranlaw.com

LE & TRAN
LAW CORPORATION

ChatGPT does warn people about what happens when they use the system.

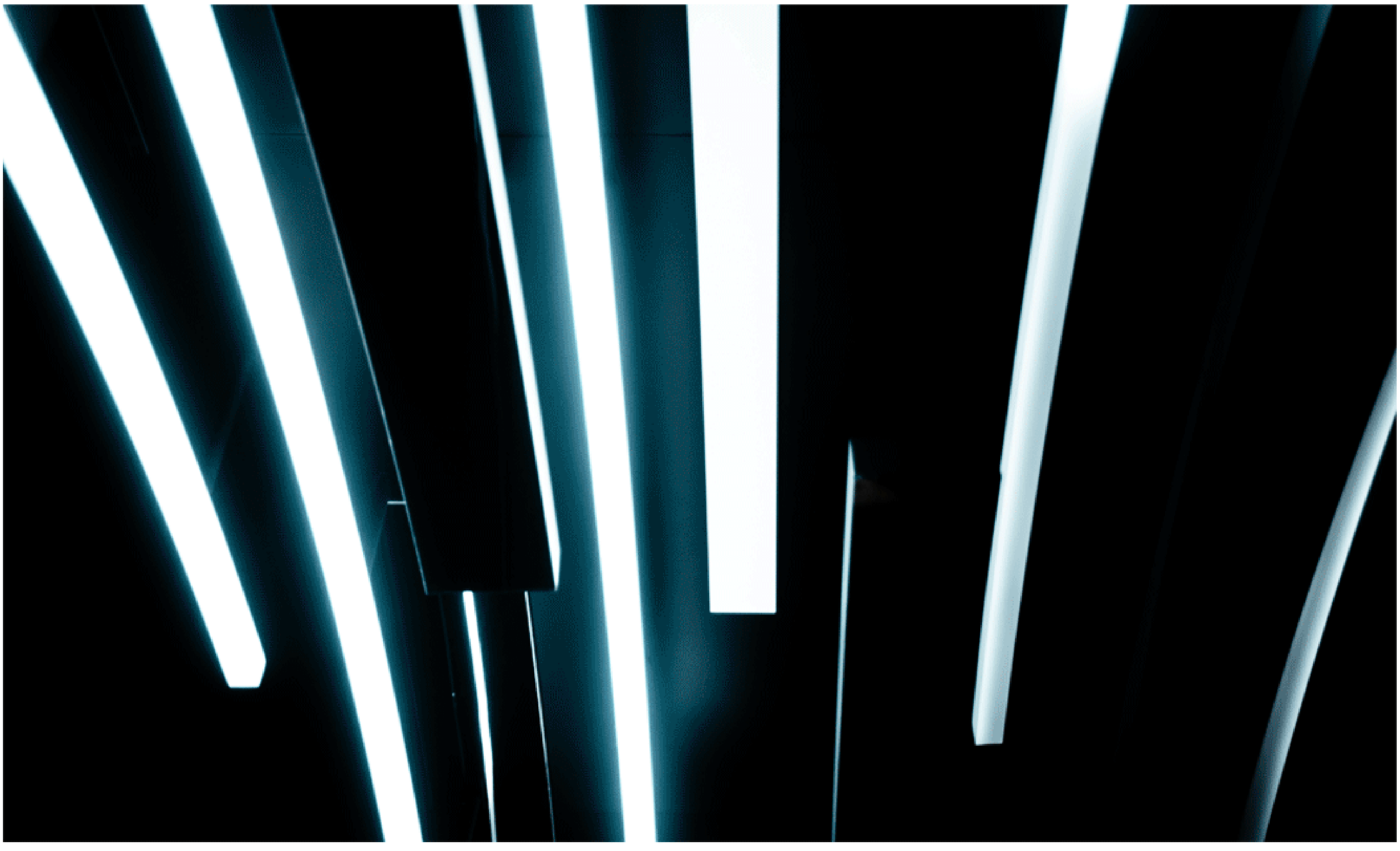
Its data policy explicitly cautions users not to share sensitive information in conversations with the chatbot, since every piece of data typed into the system will be used to train the artificial intelligence (AI) models.

It’s hard to believe Samsung’s highly-talented software engineers didn’t know the Internet could be dangerous. After all, the No 1 maxim of the Internet is: assume your session is compromised and act accordingly.

Stephen Le
www.letranlaw.com

LE & TRAN
LAW CORPORATION

Taking these events at Samsung at face value, they offer plenty of lessons for protecting critical intangible assets such as data and confidential information.



Stephen Le
www.letranlaw.com

LE & TRAN
LAW CORPORATION

Who is responsible?

In the Samsung case, neither ChatGPT nor the staff was directly at fault. The chatbot was only doing its job, as were the three software developers.

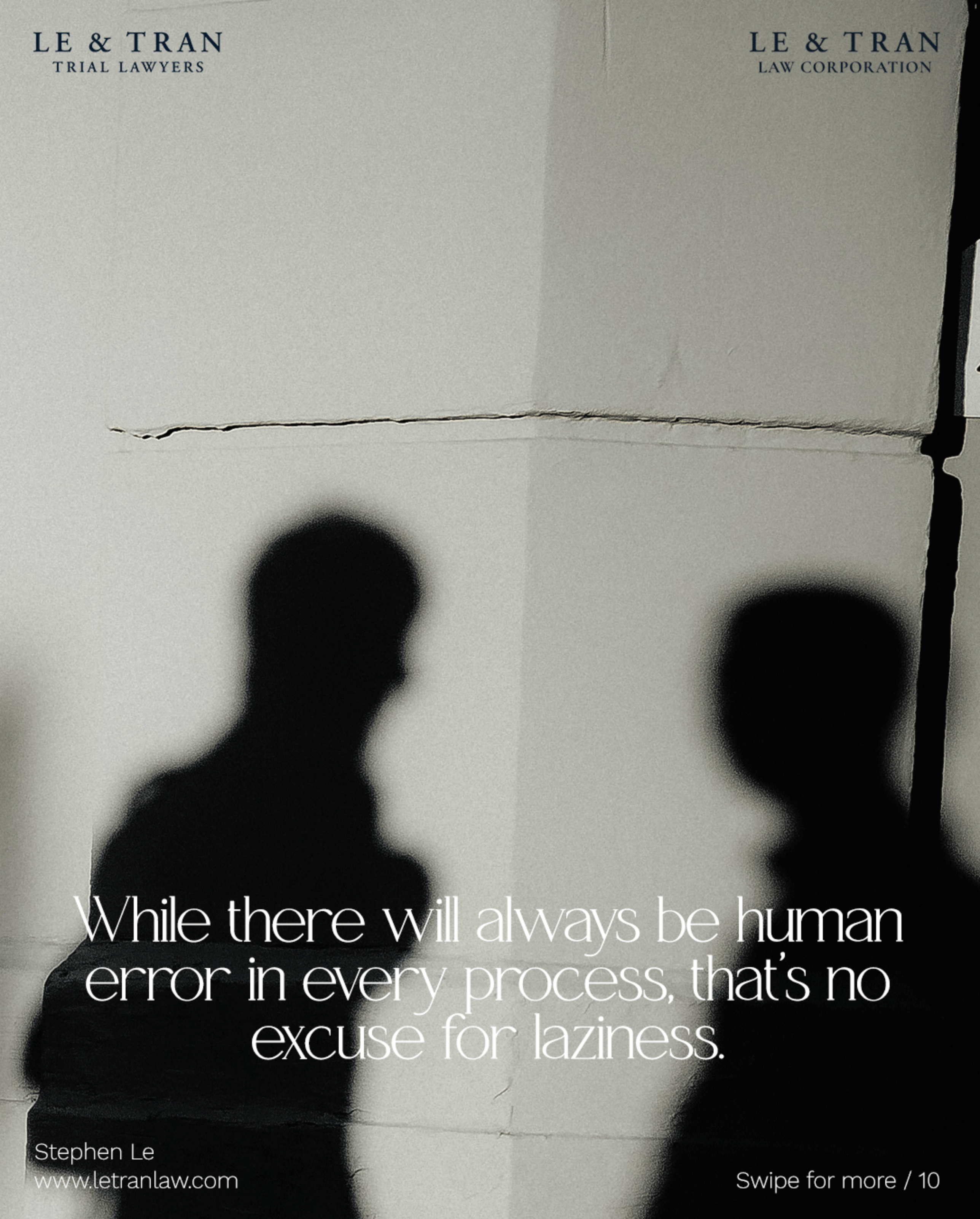
A far more effective approach is to introduce good information controls at multiple levels – including, if necessary, restricting access to services such as ChatGPT.

This approach requires that management understand the value of the company's intangible assets and create procedures to protect those assets.

Stephen Le
www.letranlaw.com

LE & TRAN
TRIAL LAWYERS

LE & TRAN
LAW CORPORATION



While there will always be human error in every process, that's no excuse for laziness.

Stephen Le
www.letranlaw.com