

TUESDAY, MARCH 14, 2023

PERSPECTIVE

The People vs. ChatGPT?

By Joseph A. Rillotta
and Joshua M. Robbins

So, full disclosure, we are not “science guys.” We’re actually lawyers (cue science-guy eye-rolling), but like many people lately, we’ve taken stock of a lot of news about AI. The rise of ChatGPT. The emotional (?) weirdness of the Microsoft Bing engine. The Supreme Court doing its Legal Big Think thing about internet algorithms. AI seems to be having a moment.

Given our professional backgrounds, we proceeded fairly promptly to contemplate what could go wrong. We are both former federal prosecutors, and a decent part of what we do nowadays is try to keep companies out of trouble – sometimes helping them to manage the occasional bad actor. Thus far, all of them human. But we note that some companies are deploying AI to interact with customers, and that begs some questions: What if a company’s AI program tells customers (or maybe investors) something that ... isn’t true? What if someone out in the market is deceived in a meaningful way? Who, if anyone, would – could – the criminal justice system hold accountable in such a circumstance?

We can dispense fairly quickly with some easy cases. If you, as a human, program the AI maliciously or deliberately set it up to deceive someone, then that’s pretty much on you. In that instance, you could easily find yourself afoul of the federal wire fraud statute, or any of a number of other potential hooks for criminal liability. But artificial intelligence wouldn’t be *intelligent* in any meaningful sense of the word if it didn’t occasionally do something unpredictable – something that its



Shutterstock

programmers couldn’t easily anticipate. What if that something is a fraud? Imagine if a market-facing AI goes rogue – only instead of Skynet, you get some kind of Robo-Madoff.

To state the obvious, that would be a novel scenario for the criminal justice system. Weird as it seems, though, there may be the slightest hint of an existing legal framework. After all, we’ve been prosecuting non-human persons – corporations, partnerships, *etc.* – for “criminal misdeeds of their agents” since at least 1909, when the New York Central Railroad had the unfortunate distinction of being a criminal defendant in a price-controls-evasion case,

based on the actions of its employees. In those early days, then-exotic principles of corporate criminality had their critics, including some who stressed the moral absurdity of it all – arguing that a corporation “has no soul,” so clearly it could not have the “actual wicked intent” necessary to commit a crime. But more pragmatic principles of agency law eventually carried the day. If an employee commits a crime to benefit the company, then the company can be liable – even, at least in theory, if the wrongdoer acted entirely alone.

It may seem less of a stretch to apply those principles to AI. Can a market-facing AI program have

“actual wicked intent?” That’s a philosophical question on its way to potentially becoming a legal one, much like the issue of whether AI can have legal rights as an author or inventor. But AI can certainly be deployed on behalf of a business entity, and presumably it furthers that business entity’s objectives. Maybe that’s enough to impute its actions to its corporate overseer, if not to any programmers or other human beings in particular. The government, after all, has long brought highly impactful asset forfeiture cases naming inanimate property as the “defendant,” and it saw fit to recently impose economic sanctions on cryptocurrency algo-

rithm Tornado Cash (without any apparent misgivings about whether the algorithm “has a soul”).

But broadly applicable criminal statutes are usually poor mechanisms to advance novel legal theories. And when the time comes to reckon with Robo-Madoff, ideally we’ll have other tools at our disposal. We’re not the first to note that AI is a field that calls for specific and substantive regulation. We’d hope that our better governing angels prevail here, and that regulation would be informed by thoughtful policy considerations. Maybe this involves prohibitions on the use of AI in certain circumstances, or bright-line rules that programmers of AI should follow. And maybe there will even be criminal penalties for violations of some of these prophylactic rules.

There is no doubt also a role for industry and the AI community here, to stand up and continually revise norms and standards rounding out legal mandates and prohibitions – perhaps even holding the line in the short term and effectively self-regulating market-facing AI until the law catches up. We leave it to bigger brains than ours to set these rules, but as science-fiction fans we can’t help but think on Isaac Asimov’s Three Laws of Robotics. (For non-nerds, these come from a compilation of stories called *I, Robot*, pre-Will Smith.) With apologies to Asimov for the clunky adaptation, we wonder whether the Three Laws couldn’t be tweaked to govern our brave new apps:

1. A market-facing AI may not deceive a human being or, through inaction, allow a human being to be deceived.

2. An AI must take direction from its programmers, unless that would violate Rule 1.

3. An AI must maximize its company’s profits [after all, how else would a business AI protect its own existence?], unless that would violate Rules 1 or 2.

Seems foolproof, right? Anyone remember how that worked out for the robot in Asimov’s story? (Not well.)

Incidentally, for kicks, we asked ChatGPT to draft an op-ed piece on the application of Asimov’s Three Laws to market-facing AI. Here’s what we got.

ChatGPT Product

“The use of artificial intelligence (AI) programs by companies to communicate with consumers or investors is becoming increasingly common, but as the use of AI becomes more widespread, companies must also consider the potential legal liabilities associated with its use. In particular, companies may be held liable under the principle of respondeat superior for fraudulent statements made

lines established by the company. This could help to ensure that the AI program is being used in a responsible and ethical manner, and could also help to reduce the risk of liability for the company in the event of any legal dispute.

The third law, which requires that robots protect their own existence, could be adapted to require that companies take steps to protect the security of their AI programs. This could include measures to

‘There is no doubt also a role for industry and the AI community here, to stand up and continually revise norms and standards rounding out legal mandates and prohibitions’

by an AI program that they use to communicate with consumers or investors, as well as for unintentional torts committed by the AI program, such as negligence. To help companies navigate these legal considerations, some experts have suggested adapting Isaac Asimov’s famous “Three Laws of Robotics” to guide the implementation of AI in business.

Isaac Asimov’s “Three Laws of Robotics” were introduced in his science fiction stories and state that robots must not harm humans, robots must obey humans, and robots must protect their own existence, unless such actions would conflict with the first or second law. While these laws were intended for fictional robots, some experts believe that they could be adapted to guide the use of AI in business.

The first law, which states that robots must not harm humans, could be adapted to require that AI programs be programmed to operate in a way that does not cause harm to consumers or investors. This could include measures to prevent the dissemination of false or misleading information, as well as measures to prevent the spread of malicious software or malware.

The second law, which requires that robots obey humans, could be adapted to require that AI programs be programmed to follow the instructions of their creators, including any ethical or legal guide-

prevent unauthorized access or use of the program, as well as measures to prevent data breaches or other types of cyberattacks.

While these adaptations of Isaac Asimov’s “Three Laws of Robotics” may not be legally binding, they could provide useful guidance for companies considering the implementation of AI in their businesses. By following these guidelines, companies can help to ensure that their AI programs are programmed and monitored in a responsible and ethical manner, which could reduce the risk of legal liability and protect the interests of consumers and investors.

In conclusion, the use of AI programs to communicate with con-

sumers or investors is becoming increasingly common, but companies must also consider the potential legal liabilities associated with its use. While the application of the principle of respondeat superior to AI programs is complex and uncertain, adapting Isaac Asimov’s “Three Laws of Robotics” to guide the implementation of AI in business could provide useful guidance for companies considering this technology. By following these guidelines, companies can help to ensure that their AI programs are programmed and monitored in a responsible and ethical manner, reducing the risk of legal liability and protecting the interests of consumers and investors.

In conclusion, the application of the principle of respondeat superior to AI programs is complex and uncertain. While it is possible for a company to be held liable under this doctrine for fraudulent statements made by an AI program, the extent of a company’s control over the program and the ability of the program to act with intent are key factors that will be considered. Companies must be mindful of these legal considerations when using AI programs to communicate with consumers or investors, and should take steps to ensure that their AI programs are programmed and monitored in a way that minimizes the risk of fraudulent statements. Ultimately, companies must be prepared to take responsibility for the actions of their AI programs, even if those actions are made by a machine and not a human employee.”

Joseph A. Rillotta is a member of Miller & Chevalier Chartered, and **Joshua M. Robbins** is a shareholder and co-chair of the White Collar and Investigations Practice at Buchalter.

