



Health-ISAC Weekly Blog -- Hacking Healthcare™

Hacking Healthcare™

TLP:WHITE

Alert ID : 69a6de60

Mar 06, 2024, 03:41 PM

This week, *Hacking Healthcare™* a speech given by the U.S. Department of Justice's (DOJ) Deputy Attorney General Lisa Monaco, which outlined the DOJ's new policy to address AI-enabled or AI-augmented cybercrimes. We break down what was said, highlight a few outstanding questions, consider the policy's potential effectiveness, and ponder its potential global impact.

Welcome back to *Hacking Healthcare™*.

DOJ Signals Intent to Treat AI Use in Malicious Acts as Aggravating Factor in Sentencing

AI is understandably a hot topic of conversation, with government and industry figures even referring to it as the "steam engine of the fourth industrial revolution."^[i] Within cybersecurity circles, optimism over how AI might aid network defenders has generally been overshadowed by concerns over its deployment by malicious actors. A recent talk by Deputy Attorney General Lisa Monaco spoke to both sides of that conversation and provided an interesting view into how the current Department of Justice is thinking about prosecuting AI-aided or -enabled cyberattacks.

Speaking at the University of Oxford on February 14th, Monaco said she is "laser-focused on what may well be the most transformational technology we've confronted yet: artificial intelligence, and what it portends for our core mission."^[ii]

Identifying AI as a double-edged sword, Monaco outlined the good it may do by noting its "potential to be an indispensable tool to help identify, disrupt, and deter criminals, terrorists, and hostile nation-states from doing us harm." However, she also acknowledged that AI is "accelerating risks to our collective security," including its ability to "amplify existing biases and discriminatory practices, ... [accelerate] the spread of disinformation and repression ... [and] lower the barriers to entry for criminals."^[iii]

A New Legal Regime for AI?

One aspect of Monaco's talk was to liken AI to the legal evolution around cyber more generally and to support the notion that while new governance approaches and laws for AI will be needed, a strong legal foundation already exists. Her speech essentially reiterated that many of the concerns over how AI might

be used in malicious acts are not inherently new and thus could be addressed with existing laws. Monaco highlighted that “[d]iscrimination using AI is still discrimination. Price fixing using AI is still price fixing. Identity theft using AI is still identity theft.”^[iv] In these terms, and noting that, “like a firearm, AI can also enhance the danger of a crime,” the DOJ appears to view AI as more of an element that may exacerbate malicious crimes and activities.

As such, Monaco made it clear that where AI amplifies offenses, the DOJ may seek to impose more significant sentencing, saying:

“Going forward, where Department of Justice prosecutors can seek stiffer sentences for offenses made significantly more dangerous by the misuse of AI – they will. And if we determine that existing sentencing enhancements don’t adequately address the harms caused by misuse of AI, we will seek reforms to those enhancements to close that gap.”^[v] In her mind, “This approach will deepen accountability and exert deterrence. And it reflects the principle that our laws can and must remain responsive to the moment.”^[vi]

Action & Analysis

****Included with Health-ISAC Membership****

Upcoming International Hearings/Meetings

EU

- European Parliament - Committee on the Environment, Public Health and Food Safety (3/11)

US

- No relevant meetings at this time

Rest of World

- Health-ISAC APAC Summit (3/19 - 3/21)

^[i] World Economic Forum: Davos 2024. Generative AI: Steam Engine of the Fourth Industrial Revolution?

^[ii] <https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-university-oxford-promise-and>

^[iii] <https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-university-oxford-promise-and>

^[iv] <https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-university-oxford-promise-and>

[v] <https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-university-oxford-promise-and>

[vi] <https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-university-oxford-promise-and>

[vii] <https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-university-oxford-promise-and>

Report Source(s)

Health-ISAC

Reference | References

[US Department of Justice](#)

Tags

Hacking Healthcare, Department of Justice, Department of Justice (USA), Department of Justice (DoJ), Cybercrime, AI, Artificial Intelligence, law

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions and/or Comments:

Please email us at contact@h-isac.org

Conferences, Webinars, and Summits:

<https://h-isac.org/events/>

Hacking Healthcare[®]:

Hacking Healthcare is co-written by John Banghart and Tim McGiff.

John Banghart has served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Council's efforts to address significant cybersecurity incidents, including those at OPM and the White

House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Council's Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

Tim McGiff is currently a Cybersecurity Services Program Manager at Venable, where he coordinates the Health-ISAC's annual Hobby Exercise and provides legal and regulatory updates for the Health-ISAC's monthly Threat Briefing.

- John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.
- Tim can be reached at tmcgiff@venable.com.

Access the Health-ISAC Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

For Questions or Comments:

Please email us at toc@h-isac.org