Interview with Miles Brundage and Shahar Avin
March 5, 2018

Overview
In our 206th episode of The Cyberlaw Podcast, Stewart Baker, Maury Shenk, Megan Reiss and Gus Hurwitz discuss:

- Evaluating the oral argument in Microsoft's Ireland case.
- Google issues a report on how it's implementing the Right To Be Forgotten.
- The Securities and Exchange Commission issues cybersecurity guidance.
- CFIUS: Chinese bodies keep piling up:
  - Xcerra deal fails.
  - Cogint fails too, and Genworth is on the bubble.
- Next steps in attribution: false flags at the Olympics.
- Facebook, Google get one hour from the European Union to scrub terror content.
- Related: Section 230 "platform" immunity begins to fray in the land of its birth.
  - Why this will end in tears.
    - The story.
    - The apology.
- Blurred line between criminal and state cyberespionage.
- Edward Snowden criticizes Apple for posing as a protector of privacy while actually cozying up to a dictatorship. Words fail me.
- Should we be worried about interstellar hacks

Our guest interview is Miles Brundage, AI Policy Research Fellow at the Future of Humanity Institute at Oxford and Shahar Avin of the Centre for the Study of Existential Risk and Research Associate at Cambridge to discuss their newly released paper The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Mitigation.

As always The Cyberlaw Podcast is open to feedback. Send your questions, suggestions for interview candidates or topics to CyberlawPodcast@steptoe.com or leave a message at +1 202 862 5785.

The Cyberlaw Podcast is thinking of hiring a part-time intern for our Washington, DC offices. If you are interested, visit our website in the next week or so at Steptoe.com/careers.

Download the 206th Episode (mp3).

Subscribe to The Cyberlaw Podcast here. We are also on iTunes, Pocket Casts, and Google Play (available for Android and Google Chrome)!

The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.

Practices
Privacy & Cybersecurity