

Cybersecurity Breaches and Private Law – Taking Stock and Looking Ahead

Title: Liability Meets Self-Thinking Toasters: The IoT Supply-Chain Liability for Cyber and AI Risks

Name: Omri Rachum-Twaig

Institution: Cyber & Information Technology Practice, Fischer Behar Chen Well Orion & Co

Abstract:

In the age of IoT and robotics, the cyberspace is no longer limited to bits and bytes. Connected devices and personal use robots allow the cyberspace to directly affect the physical space in a more concrete way than ever, not only with respect to critical infrastructures, but also at our homes, workplaces and roads. How should liability be constructed in this context? More specifically, in the context of connected products, do models of product liability fit the cyberspace framework? Should manufacturers of connected devices be strictly liable for cybersecurity breaches and any related damage? Should programmers of machine-learning robots be liable for every expected and unexpected future conduct and action of the robot? Alternatively, should we turn to alternative models for liability such as service provider liability, operator liability or even end-user liability? Choosing the most suitable liability model is dependent on understanding the risks involved, the technology itself, the protected individual rights and their underlying justifications and the potential outcomes and market effects of each model. Only by weighing these various factors, will the legislator be able to strike a balance that will provide proper deterrence and compensation mechanisms on the one hand and will not restrict the technological activity altogether on the other hand.