Cybersecurity Breaches and Private Law – Taking Stock and Looking Ahead

Title: Toying with Privacy: Regulating the Internet of Toys

Name: Dr. Eldar Haber

Institution: University of Haifa

Abstract:
Recently, toys began to play with children. The evolution of technology and the "Internet of Things" (IoT) has enabled toys to become smarter and connected: they can now interact with children by "listening" to them and respond. For children, these toys could be a lot of fun. But along with the potential benefits of these connected smart toys to some children, lies a big concern: how to protect children, especially young ones, from the capabilities of connected smart toys that could constantly collect data about them, and transmit it to other interested parties. Even more profoundly, in an age of ubiquitous surveillance, another fear arises: how to protect young children from the potential vulnerabilities of these toys which might be hacked or simply misused. In other words, do connected smart toys condition children to constant surveillance? How does the current legal framework cope with these risks? How should regulators balance between technological innovation and the need to secure children's rights and liberties? And finally, what are the implications of connected smart toys within the realm of IoT to civil rights and liberties of both children and adults?

This Article will focus on these and other important concerns that connected smart toys raise. It will proceed as follows: Part I will briefly outline the smart toys market, while exemplifying the abilities of these toys to collect and retain data. Then, using the example of U.S. legal framework which was chosen to protect children from online activities almost twenty years ago (COPPA Regulation), the next part will analyze whether it fits within the realm of IoT. Within this analysis, this part will show how key market players currently comply with COPPA Regulation through their privacy policies, and evaluate whether such compliance is even relevant in light of IoT risks and challenges. The next part will then broaden the discussion on regulating connected smart toys by discussing and evaluating the innovation-privacy conundrum. More specifically, this part will evaluate other mechanisms to regulate connected smart toys, and suggest that the current American legal framework is inadequate to properly address the risks that these toys entail. The final part will discuss the normative implications that arise from turning into an 'always on' society, and suggest that smart connected toys are a mere fraction of the risks that arise from 'always on' technologies. To mitigate these risks, policymakers must recalibrate the current legal frameworks that govern surveillance in the digital age.