The Right to Encryption – Workshop Summary

On Monday, September 23rd 2019, The Federmann Cyber Security Center – Cyber Law Program, in cooperation with Essex University Big Data and Human Rights Program, held a one-day international workshop on the Right to Encryption. The workshop aimed to investigate the question of whether there is an emerging right to encryption, what are the positive and negative obligations on states and other stakeholders in this connection and how would such a right interact with other online and offline rights, such as the right to be forgotten and the right to privacy.

The opening panel's presentation, 'Unpacking Encryption Rights', presented a conceptual breakdown of 'the right to encryption' using Hohfeldian analysis, which allows for a more nuanced approach, taking note of the corollary obligations entailed by each such encryption rights, and the relevant actors thereto. The subsequent comments considered whether encryption rights are derivative rights, suggesting that the challenge is how to encapsulate their inter-connectedness to fundamental rights.

The following presentation, 'Encryption: A Fundamental Right...But Only as Absolute a Right as Privacy Itself', expanded on the theme, arguing that there is a fundamental, however not absolute, right to encryption. The right to Privacy can be seen as an enabling right for an over-arching fundamental right to free, unhindered development of one's personality. The right to encryption should accommodate also the absolute nature of the right against self-incrimination, enabled thereby. State surveillance and decryption measures cannot be opaque to the public, and must be provided for by law, which establishes clear safeguards for privacy and clear remedies for its breach, conforming to standards of proportionality and necessity.

The third panel "The Freedom From Decryption – Case Studies", opened with the presentation "The Tech Industry's Business and Social Goals Will Undermine Its Commitment to Unbreakable Encryption", describing recent international political developments that may pave the way to weakened commercially available encryption measures. US AG Barr's recent arguments in favor of 'responsible encryption', which centered on a 'security vs. security' balancing, coupled with an encryption-limiting legislation in non-US jurisdiction, may cause tech companies to slowly lose the battle over encryption.

The issue of compelled decryption of addressed by the next presentation, “Reexamining the Privilege against Self-incrimination in Light of Recent Technological Advancement.” Examining five alternative models for the applicability of the privilege against self-incrimination within the context of compelled decryption. Under a preposition where the right against self-incrimination is relative, a model framework for compelled encryption was suggested, consisting of several thresholds (judicial warrant, lawful seizure of the device, the investigating authority must prove that the suspect remembers the password) and suggested guidelines (such as the severity of the offence, the investigative authority’s ability to independently unlock the device, or the substantive nature of the encrypted evidence).

The fourth panel, “Limits on Encryption Technology Development, Marketing and Transfer” focused on technical aspects of encryption. Its first presentation, ‘Ultimately Secured Secrets in the Quantum Era’, described the upcoming era of quantum computing, in which RSA encrypted materials may be breakable. The following presentation ‘The Official Guide to Backdooring Cryptography’, outlined the history of US government inference with encryption measures – from gag orders through key escrow programs and attempts to weaken standardization of encryption.

Concluding remarks from workshop participants highlighted themes that emerged throughout the day such as encryption as a building block of internet infrastructure and as enabler of trust; the important role of non-state stakeholders in the debate; and the need to differentiate between data in transit and data at rest. The question still remains, however, whether encryption as a derivative right is sufficient or should a free standing right for encryption be formulated