Data Protection Law and Multi-Party Computation: Applications to Information Exchange between Law Enforcement Agencies

Abstract: Pushes for increased power of Law Enforcement (LE) for data retention and centralized storage result in legal challenges with data protection law and courts-and possible violations of the right to privacy. This is motivated by a desire for better cooperation and exchange between LE Agencies (LEAs), which is difficult due to data protection regulations, was identified as a main factor of major public security failures, and is a frequent criticism of LE. Secure Multi-Party Computation (MPC) is often seen as a technological means to solve privacy conflicts where actors want to exchange and analyze data that needs to be protected due to data protection laws. In this interdisciplinary work, we investigate the problem of private information exchange between LEAs from both a legal and technical angle. We give a legal analysis of secret-sharing based MPC techniques in general and, as a particular application scenario, consider the case of matching LE databases for lawful information exchange between LEAs. We propose a system for lawful information exchange between LEAs using MPC and private set intersection and show its feasibility by giving a legal analysis for data protection and a technical analysis for workload complexity. Towards practicality, we present insights from qualitative feedback gathered within exchanges with a major European LEA.