Measuring Incidental Collection in Foreign Intelligence Surveillance

Section 702 is a surveillance authority enacted as part of the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008. It regulates surveillance conducted inside the United States that targets non-U.S. persons located outside the United States. The intelligence community (IC) element that nominates a target for Section 702 collection must have a reasonable belief that the target is a non-U.S. person located outside the U.S. However, communications involving persons located inside the United States can be "incidentally" collected if a target is party to or mentioned in the communication. Senior officials in the IC, congressional leaders, oversight bodies and civil society groups have all acknowledged the value of estimating the magnitude and properties of incidental collection. We present the first multiparty protocols with strong privacy guarantees that reliably measure the scale of this "incidental" collection of communications involving persons located in the United States. The core building block, a novel Multiparty Private Set Intersection Cardinality (MPSI-CA) protocol, is more efficient than prior work when sets are unbalanced. Our protocols are designed to protect intelligence sources and methods, and respect individual privacy.