We live in modern times when technological advances made "Big Brother" scenario feasible. By monitoring electricity consumption it is possible to rather accurately guess what people are doing in their homes - watching TV, having shower or cooking dinner. By monitoring credit card transactions a great deal can be learned about individual's traveling and shopping habits. These threats may look far fetched, but they are indeed very realistic as personal information of this kind is regularly being collected, processed and sold. However, even to most passionate privacy advocates agree that prohibiting the collection of data is not a solution, as more and more organisations and companies depend on such data for their day-to-day operation, as well as strategic planning and decision making. Thus the solution lies in promoting techniques which make individual values not only inaccessible but also impossible to infer, while at the same time allow for unrestricted use of aggregate data.

In this talk we focus on techniques for protecting the confidentiality of individual values used in statistical analysis and data mining and we show somewhat surprising connections with some combinatorial and graph theoretic concepts, including maximum antichains of finite sets and graphs with least eigenvalue -2.