The headline of the article I have read is “Credit card study blows holes in anonymity. Attack suggests need for new data safeguards”.

It is a scientific article published on 30 January in 2015. The author of the article is John Bohannon.

The author starts by telling the reader a very simple fact, which purpose is to stress the reader. The fact consists in ability to de-anonymize person having vary small amount of information, which on the first site is not correlated with the person at all. The author explains how it works in details on a specific example: using the metadata of the credit card transactions and the revealed information on taxi rides, researchers managed to rebuild transaction records by individual and to correlate it with concrete people using information on their taxi rides. The author calls such de-anonymization attack as “correlation attack”, based on a computer science.

He says that correlation attack is always possible, but the less specific information we have, the harder it is to de-anonymize the person.

As a solution for the problem author shows as an example the “safeguards”. These systems can answer the researcher’s questions having the full statistics in its depths. But instead of giving the concrete answer, they will operate with some abstracts, e.g. ranges of numbers. This will enable researchers to study big data and do their work, but it will defend from de-anonymization.

As a proof of the safeguards approach, author gives MIT database as an example of the very interesting data for education researchers, which must not be available as is, to defend students and ex-students from de-anonymization.

I found this article interesting, but before I will fully accept it, I prefer to think of another more fundamental question: “Whom we want to be protected from? And do we need to be really protected?” Only after the potential attacker will be formulated, it must be thought of protection techniques. I can’t but agree with the author de-anonymization capabilities in modern world is amazing.