

27 May 2008

By: Marius Oiaga, Technology News Editor

Sergey Yekhanin
Microsoft

[Google "Pays" Microsoft Researcher \\$20,000 to Do What It Can't](#) *Privacy award won by Sergey Yekhanin*

Google and Microsoft are unlikely partners, as the two companies have conflicting interests especially in terms of the search engine and online advertising markets. Still, the Mountain View search giant and the Redmond software company do manage to find common ground. In this regard, user privacy is one area where the duo share portions of a pseudo-common vision. Pseudo-common, because although Microsoft has set in place very strict rules regarding privacy, Google has problems adhering to a similar model. But this is not stopping the Mountain View company from looking for solutions, and not even from throwing money in the way of a Microsoft Researcher. One at [Microsoft Research Silicon Valley Lab](#), Sergey Yekhanin is the recipient of the 2007 Doctoral Dissertation Award from the Association for Computing Machinery. The award is worth no less than \$20,000, and is sponsored entirely by Google. Despite being an indisputable leader on the search engine and online advertising markets, Google has failed to take on a similar avant-garde position in terms of protecting user privacy. And due to its domination over the Internet, the Mountain View search giant is also a lightning rod for privacy concerns, which it has yet to address properly. Meanwhile, Microsoft is making headway when it comes to protecting users' privacy. Yekhanin's work is designed to safeguard the privacy of users' queries in scenarios involving public database access. A cryptography expert with the Redmond company, Yekhanin focused on a new strategy to protect and keep user queries private and detailed the model in the "Locally Decodable Codes and Private Information Retrieval Schemes" whitepaper. The annual ACM Awards Banquet scheduled for June 21, in San Francisco will act as the stage for the delivery of the Doctoral Dissertation Award. "Yekhanin's research provides a fresh algebraic look at the theory of PIR schemes and LDCs, and creates new families of PIRs and LDCs that have much better parameters than those previously constructed. For PIRs, these parameters include communication complexity, which counts the number of bits exchanged between the user and the servers, and the number of servers involved in a protocol. For LDCs, these parameters include codeword length, which measures the amount of redundancy that is introduced into the message by the encoder; and query complexity, which counts the number of bits that need to be read from the codeword in order to recover a single bit of message," ACM [revealed](#).