GCRI INTERVIEW

Prof. Dr. Jörn Müller-Quade

Head of the research group "Cryptography and Security" at the Karlsruhe Institute of Technology (KIT) and director at the Research Center for Information Technology (FZI). Spokesperson and initiator of the KASTEL competence center.

How would you describe your work for a general audience?

I am a cryptographer. Cryptography, however, has changed from looking only at ciphers, like Enigma, to the science of protecting privacy and integrity in complex distributed applications. Cryptography today covers tasks like the following: key distribution among people who never met in person, online voting with voter privacy, crypto currencies, privacy-preserving data analytics, and many more. I, personally, work on defining security (you cannot get what you want until you know what you want). Defining security has a lot of subtle issues. For example, in online voting there is no voter privacy if all participants voted for the same party, or secure communication does not hide the length of the communicated messages. If one gets the security definition wrong, the task can become impossible or meaningless. My pet topics here are security solutions, which remain secure under composition. Interestingly there are stand-alone solutions, which become insecure if carried out together. This is very counterintuitive, but an important issue if one wants to use a modular design approach to complex systems.

Complex systems require much more than cryptographic security, since IT security can only be achieved in a joint effort of many disciplines. This is why I need to cooperate with many experts from other fields, spanning from legal issues or software engineering to (quantum) physics.

In the context of Big Data, what are the benefits and risks of collecting information indiscriminately?

There are clear benefits of collecting information indiscriminately. For instance, one can use data to analyze questions that one did not even think about when collecting the data initially. One can even identify new and interesting questions. If data points are interpreted as points in a multidimensional space, one can observe that some points appear in clusters. Such clusters can yield unexpected correlations and

new questions. This use of Big Data is not possible if one has to specify a precise objective before the collection of data.

The possibility to find unexpected correlations is also the reason why collecting information indiscriminately is a huge privacy violation. Unexpected correlations are, indeed, unexpected, and it seems impossible to give an informed consent for the use of data if one cannot know beforehand what might be concluded from the data. Data collected from navigation, fitness tracking, web searches and other online services give a very deep insight into our privacy. If you don't know the purpose of the data collection, and you don't even know which different sources of data are analyzed together, you cannot judge the consequences – which could be that you might not get a certain job, loan, or insurance, or you might have to pay personalized (unfair) prices because an estimate has been made, based on your behavior, to be the maximum of what you are willing to pay. The value of privacy is, in my opinion, vastly underestimated. Data is valuable, not only for targeted advertising. Companies use data to directly increase their profit, possibly at the expense of the users.

Could you please explain what a smart environment is and what the challenges are for securing one's personal data within this setting?

In a smart environment, previously isolated appliances and devices are connected, exchange data, and are enriched with artificial intelligence.

Smart environments can be very convenient. In the future, digital assistants will sense our wishes and habits and will significantly simplify our lives. A smart environment is computer controlled, but the computers do not appear as technical entities. The interaction, e.g., via speech interfaces, feels like communicating with a concierge or a friend.

This is also a great danger as the digital assistant is not a friend, but provided by a company with its own interests and business model in mind. So smart environments, which can identify people by voice and sense our emotions, will breach our privacy in an unprecedented way and might influence us in how we make decisions (nudging).

What advice do you have for individuals who want to protect their privacy without giving up online social networks?

Privacy is difficult to keep if one is participating in online social networks. Still one can do some things (e.g., try to select a privacy-friendly provider), but this might be difficult due to peer pressure. Use the privacy settings if there are any. Read the terms and conditions you are agreeing to – even though these are intentionally formulated in a way to make it hard to understand the real consequences (e.g.,

who owns the right to pictures uploaded by you or which data might be sold to third parties). If you don’t know where the data ends up, then post only what you would like the public to know. Don’t post compromising photos or the dates when you will be away from home for long (there has been a service called “please rob me” collecting information about empty homes via social media).

Are protection attempts like "the right to be forgotten" in the European Union enough for online users to regain control of their online fingerprints?

The European General Data Protection Regulation is a very important step towards regaining control over our data, e.g., biometric data like fingerprints. But not all companies (or states) comply with laws. Hence, at least equally important are technical means to protect our data. We need research to clarify to which extend we can have a digital sovereignty by technical means.