Getting out of the digital trust trap

Thomas Kremer - Board member for Data Privacy, Legal Affairs and Compliance.

Sep 20, 2016

Silicon Valley's dominant companies, those Internet giants, present us with a contradiction. On the one hand, users love their services, and thus their business models have been wildly successful. On the other, users don't consider the companies particularly trustworthy. Even in the United States, surveys find that people are increasingly concerned about how their data are being handled, and many people have even stopped using the Internet.

This is a dangerous trend. It's dangerous of course for the companies whose business models are built around data analysis. But it's also dangerous for our economy and for our society as a whole. This is because it threatens digitization's potential to improve our lives. For example, digitization can improve traffic safety, since the self-driving cars it is bringing are immune to human failings such as distraction, fatigue and drunkenness. And with its ability to leverage big data, it can lead to the development of better medical treatments.

The progress of digitization depends on people's trust. And people's trust can be undermined by companies and overly ambitious security policymakers alike. There are many ways in which we can strengthen people's trust. First of all, we have to remember that there can be no trust without transparency. People must be able to know how their data are being used, and they must be able to consciously decide whether or not to accept such use. For example: data privacy information now run to an average of 2500 words – 2500 words that just about no one reads. Such notices need to be clear, concise summaries. This is why Deutsche Telekom has now trimmed its data privacy information down to a maximum of one page.

But transparency alone is not enough. We also need systems that can reliably anonymize or pseudoanonymize data in all cases where no direct personal reference is required. This would apply, for example, to data collected in connection with local public transportation. In Europe, the General Data Protection Regulation gives us a good basis for combining digital business models with high data privacy standards. We now need to ensure that such standards enter into force around the world.

Secure encryption also helps to build customer trust. Use of reliable encryption must be assured in connection with any sensitive personal data such as health data. However, processing of encrypted data is still out of reach. New methods of "homomorphic encryption" need to be developed to make such processing routine. Proposals for

furnishing security authorities with "spare keys" or "back doors" are counterproductive. Such keys or doors would quickly be exploited by criminal elements. They would thus undermine efforts to enhance security.

We also need smarter solutions in the area of cyber security. As attacks become increasingly sophisticated, it is not enough to simply make walls ever higher. We need to detect attackers – for example, with techniques that identify unusual behavior in the network. Needless to say, security solutions have to be easy for customers to use. Otherwise, they will not be accepted.

It is indeed true that we in Germany and Europe tend to be more concerned about the ways our personal data are used. In 1983, Germany's Constitutional Court issued its "census judgment," which established a fundamental right to "informational self-determination." The public debate at the time was similar to much of our modern discussion in that it pitted concerns about data privacy against concerns about increasing security in the face of a threat (in that case, a terrorist threat). Policymakers today need to refrain from enacting short-sighted measures that could endanger any sensitive balance we have achieved between these two areas. We now have the opportunity to ensure that the digitization of our society is a success. Europe's high data privacy standards are an advantage – not a disadvantage – for our efforts to bring about such success. Nonetheless, our companies need to considerably intensify their own efforts in these areas. At the moment, fortunately, it seems that America's big West Coast players are understanding this.

Dr. Thomas Kremer is Member of the Board of Management of Deutsche Telekom AG for Data Privacy, Legal Affairs and Compliance. In cooperation with the Munich Security Conference, the company is sponsoring the Cyber Security Summit. The range of issues covered by the Summit, which will take place on September 19 and 20 in Silicon Valley, will include innovations and a global legal framework for data privacy and data security.