# ILLUSION OF SECURE INFORMATION SOCIETY

We are living in the midst of an information age, and the majority of people think that their data is much more safer than it was in the past. Actual point that is often overlooked is that we can never be sure that our data is secure because we entrust our data to certain big tech companies, and technologies we use today are mostly developed by these companies. If the developed security technologies for handling our data are not monitored by computer professionals, this may lead to a situation in which our data can be used for any purpose. Computer professionals should handle three main issues to prevent such computing dystopia; Development of universal security policies, development of open-source cryptographic algorithms and protocols, and informing the public consistently related to security issues in information technologies.

First issue to be handled by computer professionals is the development of security policies which should be applied universally as a ground truth. These policies should be monitored by assigned computer professionals because companies which claim to obey these policies may be distorting them in fact. For instance, many companies put cookies on their websites by claiming that they will offer you more personalized offers in your subsequent visits by actually knowing you, but we can only be sure that they are not using this information for another purpose if they are tracked by computer professionals in this process. Indeed a universal set of policies to be applied is a requirement for establishing trust and preventing malicious uses of personal data.

Second issue to be handled is the development of open-source cryptographic algorithms and protocols. Cryptographic algorithms are used to encrypt our data for ensuring secrecy, so standards for the development of these algorithms should be made public so that computer professionals from all around the world can contribute to development and ensure the real functionality. Along with the previous reason any non-expert peoples can also have a right to know how their data is kept secret and secure. Unfortunately, development of such open-source cryptographic algorithms is not solely sufficient; protocols which use these algorithms as their building blocks should also be designed in the same open-source contribution way in order to ensure that developed algorithms are actually applied in real-life applications. In brief development of open-source cryptographic algorithms and protocols are indispensable for establishing secrecy for everyone without depending on certain companies for developing these standards and giving everyone the right to know how their data is kept secure.

Third issue to be handled is providing all the citizens of an IT configured society with relevant information to become aware of threats that can be encountered in daily life scenarios. To achieve this purpose, informative seminars related to information security which are not very technical but useful should be given by computer professionals. These seminars have to be consistent in order to keep the public alert and knowledgeable regarding advancing security measures and emerging hazards. In short, apart from the development of unanimous standards, public awareness of these technologies and policies should be maintained at a high level in order to prevent people from getting deceived.

In conclusion, in order to prevent possible security breach dystopia, three main issues should be handled by computer professionals which are development of universal security policies, design of open-source cryptographic algorithms and protocols, and conveying these developments to the public on a regular basis. If these issues are not handled it will become inevitable for society in which personal data of anyone can be used by big tech companies or malicious third parties for any purpose.