Suggested Resolutions For Big Data Analytics Issues

We can infer that the surveillance practices and principal changes in surveillance activities are increased by the use of big data analytics. To solve the problem, prohibiting large amounts of data collection is more likely to be unrealistic option so we should find an alternative way to allow authorised use of big data and protect our privacy at the same time, which can make our lives much easier, secured, and more productive.

For instance, by using secured and authorised big data technology, people can stop worrying about stolen identities and possible financial loss as it has a significant improve on the efficiency of fraud detection. Therefore, to preserve the integrity of human rights controlling and defences, guidelines for the use of big data analytics should be developed in human rights. The main key to control the influence of big data is transparency, while addressing its security and privacy challenges. Information on what data is gathered, for what purposes, how the data is stored, who has access to it and how that access is granted should be attached. Users must be aware of the whole process. By providing such information about the security controls used in big data companies for how they protect the data they manage, can earn public trust. In case of china's social credit system, people need to trust individuals within government or in general whoever is controlling the system. Controllers should provide transparency by reducing ambiguity and vagueness of the algorithms, so that the citizens make sure that their ratings and data are used responsibly and with their permission. The issue that could arise now is that the system could be hacked and securely threatened if the information about how it works is known.

However, It is crucial to have transparency in how the scoring works, if human ratings could have a drastically impact on their lives. Another technique can be used to protect large companies' data from being hacked and if hacked, is called data anonymization. Anonymizing the data assures that all sensitive data are eliminated from the set of records gathered before initiating data analysis and processing, while preserving its format and data type. Individuals should be able to access, manage, and have control over what personal data companies collect from them and how their data is being used and shared.

The collection, use and disclosure of personal data has to be done within the frame of its purpose. Transparency and individual control must be provided, if companies will use or share personal data for other purposes, by attaching these other purposes at the time of data collection so that the user is fully aware and has a control over the data he is providing. In addition, it should be possible that companies offer a way to individuals to withdraw or limit their agreements for the terms and conditions that is used as a method for granting consent in the first place. Set reasonable boundaries on the personal data that companies gather and preserve. Only personal data needed to complete purposes specified should be gathered.

Any personal data that is no longer needed, should be safely disposed, unless they are under a legitimate obligation to do so. Companies or organisations should provide security and responsible managing of personal data. Privacy and security risks accompanied by companies' personal data practices should be evaluated carefully by companies and provide practical protections to control risks such as unauthorized access, use, destruction, or modification and improper disclosure. Companies should use practical methods to ensure they preserve accurate

personal data.

Furthermore, they should provide individuals with access to their personal data that they gather or preserve about them as well as a suitable way to give them the possibility to correct their erroneous data or request its removal or use limitation. To avoid any unplanned usage of sensitive data, tracking the movement of data within the organisational network should be possible. Moreover, to prevent the risk of malicious users, companies should define accessibility to those who works on company’s sensitive data.