

opinion paper 2

ISEC 3050 – ETHICS AND LAW IN DATA ANALYTICS



December 14, 2020

JAMIE LU

W0441213

# Statement:

“Given that encrypted technology and applications are being used to hide criminal and terrorist activity, then be it resolved that-every communication technology or device that is sold, or offered for free of charge, as a product, or offered as a service, in any of the Five-Eyes countries (Canada, USA, UK, Australia, New Zealand) must provide Law Enforcement agencies access to unencrypted data in these products or services, subject to a properly authorized warrantor or they will not be accessible in the Five-Eyes countries.”

It is quite difficult to choose a side for this statement. It is an argument of “safety” vs “privacy”, and I have the quotes there on purpose as either choice can easily be abused for personal gain. In the times we are in right now, with technology playing a large part in the operations of violence and threats, you would think that safety would take precedence over privacy. In truth, it should, anything that is for the greater good should take precedence, and this should mean that law enforcement should have access to data in these technologies, but this is more complex that it looks.

It is important to remember the power of technologies and data in the current temporal and spatial domains. Thus, ensuring the privacy of these should not be taken lightly. One can even see the shift of ethical framework when the Edward Snowden incident occurred. It was found that there was mass online surveillance and it sparked debates and even encouraged the creation of technical measures to protect confidentiality. (Runnegar, 2017)

The given statement tries to create a remedy for possible abuse of power by proposing to have a properly authorized warrantor. However, this is still quite problematic as it must be determined who this warrantor is and who gets to appoint this warrantor.

It is also unethical to prevent access to technologies that will not provide law enforcement these data because it goes against the ethical principle, autonomy.

Saying yes and granting access could have more repercussions than expected. Ethical decisions will always make the situation better and improve it. There is no guarantee that affirming the given statement will resolve more issues than it creates.

In an idealistic world where people do their jobs properly and without corruption or malice, this question would get an easy yes, but realistically speaking, it is just not viable. People can easily be corrupted and unless this issue is resolved, my answer would stand at a no.

# References

Runnegar, C. (2017, October 26). *Encryption and Law Enforcement Can Work Together*. Retrieved December 14, 2020, from Internet Society: https://www.internetsociety.org/blog/2017/10/encryption-law-enforcement-can-work-together/