Digital Surveillance

Author

Institution

Digital Surveillance

The issue of Digital Surveillance has long been debated in the public and private domains. The main query revolves around the idea of how data is collected and the use of the data collected. Already, it is a well-known fact that governments and private corporations conduct digital surveillance. By definition, digital surveillance is when companies or governments monitor activities conducted using smart devices including the smartphone and the computer (Jones, 2015). Activities that might be monitored include data being transferred between devices and even data stored in the device and on the network. Essentially, surveillance is done to acquire information about the individual; in most cases, the individual is not aware that he is being monitored (Jones, 2015). This essay will focus on ways that an individual might be tracked by digital surveillance on an average day.

Digital surveillance can be conducted using a wide array of devices. One of the most common device is the Closed Circuit Television (CCTV); this device can be used by any organization including small business to a huge government organization. The device is a great way to keep track of a person's activities; most organizations use them to keep track of reporting and departure times of employees and also to ensure that the employee is carrying out assigned tasks appropriately (Bigo, 2016). Other devices that can be used include the mobile phone and the computer. Some companies have been known to assign their employees with trackable phones for easier monitoring. Companies and governments can also tap into mobile phones as a means of digital surveillance (Bigo, 2016). Other devices that have been used in digital surveillance include biometric systems, loyalty cards and internet cookies.

The devices mentioned above can be used to collect different types of data as part of the surveillance. For example, internet cookies help collect data such as websites that are visited regularly. The mobile phone can be very helpful in collecting information such as the

number of emails sent and received (Bigo, 2016). Tapping into the mobile phone is one of the most effective means of digital surveillance since a lot of data can be collected. For instance, one can view the name of the email sender and the contents of the email. Also, one can monitor social media activities and even the location of the mobile phone (Jones, 2015). Other types of information that might be collected include credit card transactions, online purchase information, and even the types of videos one watches regularly.

As now evident, there is a wide range of information that can be collected through the use of digital surveillance. So, the question arises; to what extent can a person reject or resist digital surveillance? The digital age has brought about new security threats that have necessitated the use of digital surveillance to counter these threats (Bigo, 2016). So, what level of surveillance should be considered tolerable? Some companies have empowered people to resist digital surveillance by allowing them to choose the information that they want to share and that which they want to keep private (Bigo, 2016).

Nonetheless, the extent to which a person can resist digital surveillance is limited. The reason is that governments have to monitor people to counter security threats such as those posed by terrorists and cybercrimes that risk national security (Bigo, 2016). Also, companies have to monitor different transactions for the smooth running of the organization. For instance, credit card companies have to monitor credit card transactions to ensure the security of the buyer and that of the seller (Jones, 2015).

References

Bigo, D. (2016). Digital surveillance and everyday democracy. *The Routledge International Handbook of Criminology and Human Rights*, 151-161.

Jones, R. H. (2015). Surveillance. *The Routledge handbook of language and digital communication* (pp. 422-425). Routledge.