Unit 1 Reflective Activity – Ethics in Computing

It is fair to say that Ethics should play a part in everything that we do, and that it should be a guiding principle for how we live our lives. With modern IT technology, now at a level where it is pervasive, Stahl et al (Stahl et al, 2016) state that "we are now at a point at which computing technologies and devices pervade most aspects of personal, organisational, and social life". Ethics need to be at the forefront of our minds regarding ethical and social issues in modern society.

One such area, where there is intense focus is on data protection and confidentiality. Modern life often necessitates the use of Computers/Mobile Phones etc, for work, to book appointments at the Doctor, e-commerce sites used to order food or clothes online, or for normal e-services activities such as managing bank accounts.

Stahl et al, found that through their survey, Privacy was identified to be "the dominant ethical concern and concept employed throughout the discourse" and go on to say "privacy can be seen as intrinsically morally valuable, or derive its value from related rights or ethical concepts, often autonomy or freedom". They identify data privacy and personal privacy as the two main forms related to computing technologies.

In addition to the personal privacy issues that are at stake, there are now many legal responsibilities are regulations that must be followed in the different jurisdictions around the world. Not every jurisdiction has the same rules, and it can get quite complicated, but failure to comply can have severe legal implications for companies or people involved.

For example, the European Union has for a long time had defined rules for data privacy and sharing, recently updated to become the modern General Data Protection Regulations or GDPR (GPDR, ND). GDPR defines that data protection within the EU member states, is a constitutionalised fundamental right. This stance is mirrored, at least for now, in the United Kingdom, with their own implementation of GDPR called UK-GDPR (UK-GDPR, ND). Through a equivalency level known as "adequacy" there are broad similarities between the EU and the UK, which means that data should be protected in both jurisdictions through the same type of regulations.

Conversely however, the United States does not have any equivalent Federal rules or regulations, explicitly protecting personal data, and only a few select States have implemented these regulations (Celeste et al, 2020). This can cause problems where for example, the GDPR expects a certain level of protection, but within the US, these safeguards either do not exist or may not necessarily apply.

With many Enterprise Businesses, moving all or part of their data to the CLOUD, this problem is greatly increased, as the host CLOUDs may not be in the local jurisdiction and held accountable to those particular standards (Kushwaha et al, 2020).

So, how do we protect personal data; what can be done??

- For data that is to be shared by a company, it is mandatory that the local jurisdiction rules are complied with 100%, for example the GDPR in Europe. This is the responsibility of the Company that holds or collects the data. Storing this data in an anonymised manner in the past would have been

sufficient, but with modern IT, the previous guarantees are no longer sufficient (Kushwaha et al, 2020).

- Any data to be shared, where appropriate, should have explicit informed consent to do so. Only the data necessary to be shared, should be shared (Fitzgibbon, 2017).
- Independent oversight of a company's data privacy policy should be performed, to ensure that it is fit-for-purpose, and is being followed properly.
- Any sharing of data, must only be done with explicit consent from the user, and they must be able to withdraw consent at any time.
- Try to ensure that any sharing of data between jurisdictions, is shared to jurisdictions with similar levels of protection.
- If the Enterprise is implementing CLOUD Technologies, then care needs to be taken when selecting the regional CLOUDs where the data is stored, to ensure that they are in regions with similar rules.
- Ongoing diligence and evaluation to ensure that the regulations are continuously being followed.

References:

Celeste, Edoardo. Fabbrini, Federico. (2020). Competing Jurisdictions: Data Privacy Across the Borders. Available from: https://link.springer.com/chapter/10.1007/978-3-030-54660-1_3
[Accessed 22 October 2023].

Fitzgibbon, Mike. (2017). The Responsibility to Protect My Data: Ethical Shortcomings of Digital Data Gathering and Use in Emergencies and Development Contexts. Available from: https://pdf.sciencedirectassets.com/313346/1-s2.0-S2405896317X00037/1-s2.0-S2405896317314982/main.pdf?X-Amz-Security-Token=IQoJb3JpZ2luX2VjEON%2F%2F%2F%2F%2F%2F%2F%2F%2F%2FwEaCXVzLWVhc3QtMSJHMEUCIEXuPBxem3Re2BoLLmd7%2FhKUIcCAZQan0nL%2BeDNzksaLAiEA1xO7VPHxJPDnI9SElRsRY%2Bh74sOOB%2F2kMqixYvRDedgqsgUIEhAFGgwwNTkwMDM1NDY4NjUiDHTflR6RFq5pL0QNHSqPBa2z1y4xQrcqR8FwovMTr3kMrlhVTcUBX8O23tZ73izvJqYbxXC5%2FDRHQXdwz1du%2B8qojt2ABdIRS2yvwwsVn4f09Eq1Fov69TA2qBBEdlBP8jBXzHvWxzHIt8dHdhS2MD1OZLi2Ft3%2B66TY03052TUXJiJXOppNx1pwTappfmWKcTXUpg8HPEArw%2FXHsyG1Tet%2BSUHgSvwAJXnaNPBf%2B68lykhqYP7Wp9KW%2FXAt8ASok3i0CCr%2Fc2uFL5AvNoTNF4xg9CzCOuxI0hdEAQRBghI%2Fplx7Zq4OIwHfBH7imXYWFuD6kMGYfHdDDmIaUBgKaZ6CcBk8zPBqGEfNE%2BFjCH36HPucoMOu9HeBFQ%2F%2FIbGxLWKy8AEaJh01gmh1e0U5P2uVwHG%2BbxVzjYizqAoRBRoyc%2FjwaNncXTWXVGGwR1YNsmmss3vei%2BbeUg6Fmwye8V91HgAQILM9hlsnkBLwaNGGgcB3apUWZti%2BtN%2FgVUe9vbV3lAgZ3IB0Rezt8F4jujE4asFZc8HIeabQs6HFRObKnFmGw4vjGFYlwExjJm3d%2Fa4shBIgzvB9xA%2FK9tfmsSH21NGkUleZp0PiQNfcGJFle%2BdzFy0EPu%2FRKYvZNQVX5%2F%2BTEEn2Ctcx8N19aQxI%2BIVLd2o69kgb6UDBkWQRAw5Xe9R334RRL8njIpabR%2BCJxpvB3fbHJuKHRFMZsDhW8mD3XDnpHbcj1mGGzK1iLPkbgylSTOXqNrszA80IIR5G6M5D9eOIC6iPK7bZ6ndsKzmHr7c0Q8x8upRGmue9T7L7KHIWP3mEOm3T%2Bwli5matyCgEaRSsf%2FK3K%2FBNiR4i%2FREKw94qxrMX%2FQrZlkgQSBxVK8reHBfgvcywdr8nJ9Ywn8fTqQY6sQGCCPJUMg3E9

EiAyV8zKirYPxnQTq%2FtMYV0pvAEkNFsfOcHOTu8HsGn9NYLApM0uyPPPKOenIhFeyW3dc1%2Fh7eQDfeYOa50Jfuq7GYClPCiBGhv8EKn9tuaO%2Bi%2FGrLL7pK02iEC8JcsYrc2PtPXudVdQyPTZ2eg1i1%2FdLipo4sDhIaw0ZMh6NBOODF4eLP%2Bw%2FCbKN%2FjG5YNV3gAoXg91SFgxnZsGnfxIKnkWJL3c6BTa%2Fw%3D&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Date=20231022T093121Z&X-Amz-SignedHeaders=host&X-Amz-Expires=300&X-Amz-Credential=ASIAQ3PHCVTY52QQRYNR%2F20231022%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Signature=1f8370f9ec4c4945d9527561679956e3f0ccc39f6c4d9ff4b8d3d9bd1fa06c12&hash=893abc5fe1cf0adc008f11ff4e4e3c31f00e2970a1ea96dd8554008569272547&host=68042c943591013ac2b2430a89b270f6af2c76d8dfd086a07176afe7c76c2c61&pii=S2405896317314982&tid=spdf-62fb3c42-111d-4f1a-8515-34424b265977&sid=3e31f8642aebf54960590ba26ef043ce5861gxrqa&type=client&tsoh=d3d3LnNjaWVuY2VkaXJlY3QuY29t&ua=1b10565002570106535f&rr=81a0ba10fdb65a8c&cc=at
[Accessed 22 October 2023].

GDPR. (ND). Complete Guide to GDPR Compliance. Available from: https://gdpr.eu
[Accessed 22 October 2023].

Kushwara, Neal. Roguski, Przemyslaw. Watson, Bruce W. (2020). Up in the Air: Ensuring Government Data Sovereignty in the Cloud. Available from: https://ieeexplore.ieee.org/abstract/document/9131718
[Accessed 22 October 2023].

Stahl, Bernd Carsten. Timmermans, Job. Mittelstadt, Brent Daniel. The Ethics of Computing: A Survey of the Computer-Oriented Literature. Available from: https://dl-acm-org.uniessexlib.idm.oclc.org/doi/pdf/10.1145/2871196
[Accessed 22 October 2023].

UK-GDPR. (ND). The UK GDPR. Available from: https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/the-uk-gdpr/
[Accessed 22 October 2023].