Lecture summary of week 5 and 7

Week 5: Legal Perspectives on the Software Industry

There are two main topics in this week’s lecture: The first topics is about the legal system and discussions about fairness and ethics, and the second one is about surveillance.

Firstly, **features of the legal system** is introduced. The system can be divided into two main parts: **criminal law** and **civil law** that covers the supplementary set of criminal law. Criminal law is launched by state, so sometimes, a criminal litigation is called public prosecution. Conversely, infringement of civil law is sued by legal entities, so often those cases are referred as private prosecution. Like ethics, there is no golden rules of right or wrong, so in the court, **everything is arguable**. That’s because there are different interpretations of the rules based on the situations of each case. Law is also **sourced** from a wide variety of evidences, including: Statutes, Legislature, Codes, Jurisdiction, Precedent, Contracts, Norms and conventions.

Credibility of law is rooted in the rule of it. The fundamental nature of law is that, **no-one is above the law** which means that correctness is solely determined by the law itself, rather than somebody. And the separation of power rule **separates the power** of legislature, judiciary and execution to three independent parties to keep the neutrality of law and to restraint on arbitrary power. Under the natural justice constraint, fair judgements can be made to prevent harmful activities. Thus, companies may consider the risk of their activities as a factor to prevent the damages caused by IT failure.

To be a profession, one must adhere themselves to certain standards to meet the **professional liability requirements**. Usually, a profession needs to obtain membership from a professional body and obey some agreed standard of practice. Because being a profession not only requires professional skills, but also sets more **strict standards** on discipline and reputation. As mentioned in the lecture, Data integrity professional should also be considered due to emerging needs and the sensitive nature of data. To keep data integrity, a specific training curriculum that guarantee the disciplined professional body is required.

After that, the lecturer discussed about **dataveillance**, which raises the concern that IT companies may monitor people’s activities and collect private information with or without permission. Because there is no standard for classifying data privacy, the debates on regulation of online surveillance becomes complex. To analyse this, it is important to **avoid pre-judgement** and always make decisions base on evidence and facts. We need to focus on proper levels of oversight, proper uses of technology and proper restraints to find a balance between privacy and productivity. The most important thing to analysing is to **identify issues, strength and evidence**.

Then, ethical conundrum such as COVIDSafe app are discussed as an examples. This app detects proximity to other devices automatically to aid government contact tracing. Although it is designed with good intention, however, the evidence of actual use is unclear. And without the evidence of effectiveness, the intrusion of the app may not be legal or ethically justified. However, before widely used, assessing the usefulness is not possible. Also Big Data and predictive