References

PSI Essay
Year 3, Question 2

Anonymous Submission

March 13, 2015

1 Question

It is suggested that in the UK we are the most observed society in Europe, with a typical day in a large city involving over 300 recordings of our image on surveillance cameras. As an IT professional, one day you might well be involved in the deployment of such systems. What is your stance on the indiscriminate surveillance of the population at large? Justify your position with examples.

2 Introduction

2.1 The Benefits of Being Observed

As a highly observed society, we are subject to a number of benefits. For one, we are not subject to nearly as much crime; it is far easier to regulate a society's actions when you have video proof of everything that they do! This is not the only consideration, however. A country that monitors its people closely allows it to be aware of trends within the people. If a government can see that the people they are trying to protect are becoming more violent, or beginning to act suspiciously, then the government can research this further or intervene with actions they can predict. Particularly, the predictive power of observing people can be very useful for a government. We are constantly being reported to on the various plots that are thwarted as a result ofwo our being monitored. Certainly, safety is both an important part of modern life and of the work a government should do – however, it is my position that protecting people in this way can also introduce new risks.

3 The Risks Involved

There are two risks I would like to outline that pose potentially very serious problems to the public in the future. The first of these two risks is that the digital security of the video being recorded is often less than adequate. The second is a more contraversial view, which is that the storing of any sensitive data by the government can put its people at risk should that government become malevolent in the future.

3.1 Digital security and data loss

When we discuss the security of data in the hands of the government, certain incidents tend to spring to mind. For example, in 2013 an unencrypted usb stick was found containing sensitive data from Suffolk city council [**?**]. Data losses like this happen all too frequently – there even exists a wikipedia list of data lost by the UK government [**?**], listing 26 incidents since 2007 alone.

What can we do when our safety and privacy is put at risk? This issue is a serious one, and one that should be of great consideration when deciding exactly how much data we want our governments to attain

about us – particularly video recordings of our movements and routines, which could make us physically vulnerable.

3.2 Data Misuse

It is often claimed that, if we have nothing to hide, we should have nothing to fear if data about is is kept and stored. After all, without any wrongdoing, this could not possibly put us in any legal danger.

This is not necessarily true. It is certainly the case that, at the moment, there are legal protections that would prevent these data recordings from being used against us provided we have done nothing unlawful. However, consider that law and government change over time. There are situations where the government may use the data they have to begin to persecute people tey have protection over – a recent case would be the "Arab Spring" that took place between 2010 and 2012. During this time, "secret police" organisations would use the sensitive data held by governments in the form of web searches, emails, and even the video surveillance being discussed to target and harm people who opposed the regimes being overthrown.

Alternatively, consider areas currently controlled by ISIS, the Taliban, or Boko Haram. These places have infrastructures to collect data regarding – or at least record video surveillance of – the people being governed, and when a terror organisation overthrows these well-meaning governments this sensitive data is left available to malevolent organisations.

I am not advocating a position that the video data being collected at this moment will soon be collected by organisations like ISIS or Boko Haram. However, the possibility exists, and Britain could be a very different country in ten years time. Whether a government turn on their people, or lose access to the data they store, the people being recorded are put at risk.

3.3 The crux of the matter

A prevalent topic in current politics is gun control. An argument often put forward is that "guns don't kill people – people do". Similarly, in this situation, the collection of data itself does not expose civillians to harm – the organisations in control of this data do. If the data kept by organisations could be guarenteed to be kept safe, swathes of issues with data collection are nullified. In this way, the problems of data misuse and digital security we have discussed affect each other. If data misuse weren't a problem, its security would not matter. By the same token, if data could be verifiably secure, we would not have to worry about the collection of this data to the extent that we do now. The overlap between these two issues allows us to ascertain that we should take care to regulate the organisations in charge of collected data.

What does UK law do, then, to impose restrictions on the organisations that collect and control data from surveillance?

4 Surveillance and Law

Three laws are laid out by a LINK parliamentary report

5 Conclusion

There are benefits to collecting data regarding citizens, without doubt. It allows government to more readily organise and survey the people they set out to protect. The danger of losing the video recordings, however, is high. In one instance, it is very easy for this data to be used to target people if it falls into the wrong hands. However, if it is taken by force, or if the government are overthrown or replaced by one of less protective intentions, many people are put at risk by the recording of their lives.

How, then, do we resolve this problem? Perhaps, rather than leaning entirely into or away from surveillence, the solution is simply to strike a balance. Perhaps we mght miss a few pieces of video evidence for court cases, if the extent of the UK's video surveillance is to be lessened. With this said, in instances where court is used to persecute the innocent rather than prosecute the guilty, missing video footage could keep

people out of harm's way. We should always be striving to protect ourselves, and assuring our protection in the future is an imporant component of this.

Lastly, it ought to be noted that crime in the UK, while not at excessively high levels, is also existant. In some areas, it could even be said to be prevalent. Video surveillance can only protect people to a degree – while it will deter some crime and serve as evidence for others, it will never eliminate wrongdoing. Given that the UK is said to be the "most observed society in Europe", it might be prudent to see whether we can rely less on video footage and learn how to protect people using other means.