INTRODUCTION

We all take our privacy for granted. How much attention do you pay to the CCTV camera on your street? There is one camera for every 11 people in this country. Most roads have a camera to monitor traffic, which is legally allowed to keep recordings for up to 7 years. Your mobile phone transmits your location in almost real-time to Google and to your service provider. We store our bank details, our intimate conversations, and deepest secrets on our devices. Your bank records every transaction you make. Search engines can track almost every activity you make online. We, for the most part, understand and ignore this.

THE ACT

However, the government has recently announced a controversial bill named the 'Investigatory Powers Act. This bill, initially proposed by Theresa May as Home Secretary, and now reproposed, is claimed to put safeguards on the ability of Government organisations to gather information on citizens, while simultaneously forcing Internet Providers to store data on their users' browsing history for up to a year, and protecting the power of GCHQ and MI5 to collect bulk data.

It gives security services the power to hack into and install government-sanctioned malware on any device without alerting the owner. It has been stated that the bill effectively allows the government to view any of your files, any of your conversations, without any sign that you're up to no good. This bill, initially nicknamed 'The Snooper's Charter' when suggested in 2013, was blocked by the Liberal Democrats over concerns about the massive extent of the bill. It has now passed through the houses and received Royal assent, making it an Act of Parliament. It is proposed to help the government prevent terrorism and hate crime, but it is doubtful how effective surveillance is.

LIST OF AGENCIES

So, under this act, who can view your browsing data?

Well the list of agencies is quite extensive as you can see, but it goes on… and on… All of this begs the question, should this amount of people have access to your information? Not only is the number of people worrying, but it is also the type of people that have been granted access.

Is it really appropriate that institutions such as The Job Centre and the Welsh Ambulance NHS trust have full access to your internet history? You might reply with a niche circumstance in which they require access, but ultimately it is unnecessary.

BACKDOOR

Section 127 of the bill was particularly controversial. It obliged ISPs, telecommunications and other providers to let the government know in advance of any new products and services being deployed and allow the government to demand "technical" changes to software and systems. This is effectively allowing the government to put in place a ‘backdoor’ and deliberate security weaknesses so citizens' encrypted online activities can be intercepted, deciphered and monitored. In today’s world, encryption plays a massively important role in the function of technology most of you use regularly. Banking, social media, ATM’s, text messaging, whatsapp, and basic phone calls all depend on encryption. For the government to essentially ‘force’ these companies to include vulnerabilities leaves a lot to be questioned in how they will balance this compliance will the new bill and still managing to retain their functionality and security.

SLIPPERY SLOPE

There are some critics that say that the introduction of this act is a slippery slope that will lead to future bills being passed that grants even more access to the government. Jim Killock, the executive director of Open Rights Group, said: “The UK now has a surveillance law that is more suited to a dictatorship than a democracy. The state has unprecedented powers to monitor and analyse UK citizens’ communications regardless of whether we are suspected of any criminal activity.” This maybe a slightly exaggerated view but its message still stands. In the direction we are going with the passing of this law, it is concerning; will the extent of surveillance continue to push the boundaries of privacy?

CRITICISM AND SUPPORT

The bill was passed into law with little resistance. Many prominent MPs voted for it, and except for the odd news article expressing distaste, the vast majority of people have simply continued on with their lives, which isn’t necessarily a bad thing. The Investigatory Powers bill isn’t a black and white issue: there are clearly good aspects, and there always remains the argument that if you haven’t got anything to hide, then you haven’t got anything to fear. However, as indicated by the Edward Snowden leaks, the flow of your personal data is not always within safe hands, and privacy should always be a human right.

WAYS TO BYPASS

There are ways to bypass the surveillance. For example, by using a proxy much of your online activity can be obscured, if not entirely hidden. Some of you may even use proxies already, for privacy or other reasons. However, VPNs can be unreliable and

slow, and we have to ask if all this should really be necessary. Is it right that citizens are forced to use proxies to carry out normal activities, because of fear of surveillance? In many other countries, such as China and Iran, proxies are necessary to access much of the internet, due to government blocking. Is the Investigatory Powers Act any better than this?

THE FUTURE

There's no telling what will happen in the future. The government has officially stated that the Investigatory Powers Act is merely a kind of trial period, but, if it is deemed successful, it may or may not continue for years to come. If this is indeed a slippery slope, then we could expect much worse Government invasion to come. As the lines between preventative surveillance and punishment for thoughtcrime blur, only time will tell how far the government will go.

Thank you for listening.