**DQ1: Freedom**

In legislating on the use of computers, governments are often urged to weigh issues of security and freedom. In examining the position in the United Kingdom or a country of your choice, judge whether the correct balance has been struck, and recommend changes that you would make

1. Introduction
   1. Often times, society is presented with making a choice between freedom and security. Today, our governments tell us that in order for us to be secure, compromises in freedom must be made.
   2. Kelly et al., (2013)
      1. In June 2013, revelations made by former contractor Edward Snowden about the U.S. government’s secret surveillance activities took center stage in the American and international media. As part of its antiterrorism effort, the U.S. National Security Agency (NSA) has been collecting communications data on Americans and foreigners on a much ￼greater scale than previously thought.
      2. Of particular concern are the proliferation of laws, regulations, and directives to restrict online speech; a dramatic increase in arrests of individuals for something they posted online; legal cases and intimidation against social-media users; and a rise in surveillance. In authoritarian states, these tools are often used to censor and punish users who engage in online speech that is deemed critical of the government, royalty, or the dominant religion. In some countries, even blogging about environmental pollution, posting a video of a cynical rap song, or tweeting about the town mayor’s poor parking could draw the police to a user’s door. Although democratic states generally do not target political speech, several have sought to implement disproportionate restrictions on content they perceive as harmful or illegal, such as pornography, hate speech, and pirated media.
      3. Many governments, fearing the power of social media to propel nationwide protests, also scrambled to pass laws restricting online expression. Since May 2012, 24 of the 60 countries assessed adopted legislation or directives that threatened internet freedom, with some imposing prison sentences of up to 14 years for certain types of online speech.
   3. (Bailey, 2013)
      1. Today, eight leading Internet companies have published in several major newspapers an open letter to President Barack Obama and to Members of Congress urging them to rein in the growth of the national security surveillance state. From the letter:
         1. We understand that governments have a duty to protect their citizens. But this summer’s revelations highlighted the urgent need to reform government surveillance practices worldwide. The balance in many countries has tipped too far in favor of the state and away from the rights of the individual — rights that are enshrined in our Constitution. This undermines the freedoms we all cherish. It’s time for a change. For our part, we are focused on keeping users’ data secure — deploying the latest encryption technology to prevent unauthorized surveillance on our networks and by pushing back on government requests to ensure that they are legal and reasonable in scope. We urge the US to take the lead and make reforms that ensure that government surveillance efforts are clearly restricted by law, proportionate to the risks, transparent and subject to independent oversight.
2. 10 MOST COMMONLY USED TYPES OF INTERNET CONTROL
   1. Blocking and filtering: In 29 of the 60 countries evaluated, the authorities blocked certain types of political and social content over the past year. China, Iran, and Saudi Arabia were the worst offenders, but filtering in democratic countries like South Korea and India has also affected websites of a political nature. Jordan and Russia intensified blocking in the past year.
   2. Cyberattacks against regime critics: Opposition figures and activists in at least 31 countries faced politically motivated cyberattacks over the past year. Such attacks are particularly prevalent during politically charged events. For example, in Malaysia and Venezuela the websites of popular independent media were repeatedly subject to DDoS attacks in the run-up to elections.
   3. New laws and arrests: In an increasing number of countries, the authorities have passed laws that prohibit certain types of political, religious, or social speech online, or that contain vague restrictions related to national security that are open to abuse. In 28 countries, users were arrested for online content. In addition to political dissidents, a significant number of those detained were ordinary people who posted comments on social media that were critical of the authorities or the dominant religion.
   4. Paid pro-government commentators: A total of 22 countries saw paid commentators manipulate online discussions by discrediting government opponents, spreading propaganda, and defending government policies from criticism without acknowledging their affiliation. Spearheaded by China, Bahrain, and Russia, this tactic is increasingly common in countries like Belarus and Malaysia.
   5. Physical attacks and murder: At least one person was attacked, beaten, or tortured for online posts in 26 countries, with fatalities in five countries, often in retaliation for the exposure of human rights abuses. Dozens of online journalists were killed in Syria, and several were murdered in Mexico. In Egypt, several Facebook group administrators were abducted and beaten, and security forces targeted citizen journalists during protests.
   6. Surveillance: Although some interception of communications may be necessary for fighting crime or combating terrorism, surveillance powers are increasingly abused for political ends. Governments in 35 countries upgraded their technical or legal surveillance powers over the past year.
   7. Takedown and deletion requests: Governments or individuals can ask companies to take down illegal content, usually with judicial oversight. But takedown requests that bypass the courts and simply threaten legal action or other reprisals have become an effective censorship tool in numerous countries like Russia and Azerbaijan, where bloggers are threatened with job loss or detention for refusing to delete information.
   8. Blocking social media and communications apps: 19 countries completely blocked YouTube, Twitter, Facebook, or other ICT apps, either temporarily or permanently, over the past year. Communications services such as Skype, Viber, and WhatsApp were also targeted, either because they are more difficult to monitor or for threatening the revenue of established telecommunications companies.
   9. Intermediary liability: In 22 countries, intermediaries—such as internet service providers, hosting services, webmasters, or forum moderators—are held legally liable for content posted by others, giving them a powerful incentive to censor their customers. Companies in China hire whole divisions to monitor and delete tens of millions of messages a year.
   10. Throttling or shutting down service: Governments that control the telecommunications infrastructure can cut off or deliberately slow (throttle) internet or mobile access, either regionally or nationwide. Several shutdowns occurred in Syria over the past year, while services in parts of China, India, and Venezuela were temporarily suspended amid political events or social unrest.
3. Situation in the United States
   1. The United States has many programs which conduct surveillance on activities they deem worthy, but perhaps the most famous one is the Prism program (Kloc, 2013)
      1. PRISM is geared towards collecting the Internet data stored by nine major Silicon Valley technology companies: Facebook, Google, Yahoo, Microsoft, PalTalk, Skype, YouTube, Apple, and AOL.
      2. What data is collected? According to a slide leaked by Snowden to the Guardian and the Washington Post in early June, PRISM collects the following information from customers of the nine aforementioned tech companies: “emails”; “chat--video, voice”; “photos”; “stored data”; “VoIP”; “file transfers”; “video conferencing”; “notifications of target activity--logins, etc”; “online social networking details”; and “special requests.”
      3. How is the data collected? The program operates through a secretive judiciary body called the Foreign Intelligence Surveillance Court. The court, which was created by the Foreign Intelligence Surveillance Act of 1978, provides the agency with warrants for the private information of both foreigners and American citizens in matters of “national security.” The court has been criticized for its readiness to approve the seizure of such information. Since 1978, thousands of applications have been filed in the court. In all that time only 10 have ever been denied.
   2. The Guardian, 2014
      1. The story in a nutshell
         1. The Snowden files reveal a number of mass-surveillance programs undertaken by the NSA and GCHQ. The agencies are able to access information stored by major US technology companies, often without individual warrants, as well as mass-intercepting data from the fibre-optic cables which make up the backbone of global phone and internet networks. The agencies have also worked to undermine the security standards upon which the internet, commerce and banking rely.
         2. The revelations have raised concerns about growing domestic surveillance, the scale of global monitoring, trustworthiness of the technology sector, whether the agencies can keep their information secure, and the quality of the laws and oversight keeping the agencies in check. The agency is also required to abide by the European Convention on Human Rights.
      2. PRISM
         1. Prism is a top-secret $20m-a-year NSA surveillance program, offering the agency access to information on its targets from the servers of some of the USA’s biggest technology companies: Google, Apple, Microsoft, Facebook, AOL, PalTalk and Yahoo. The UK’s spy agency GCHQ has access to Prism data.
         2. NSA documents suggest the agency can use Prism to access information “directly from the servers” of US companies – a claim they strongly deny. Other documents showed the NSA had paid out millions of dollars to “Prism providers”, and showed Microsoft had helped the NSA circumvent its users’ encryption.
4. Issues (The Guardian, 2014)
   1. The extent to which private companies are cooperating with intelligence agencies has been a major source of concern for internet users across the world. The technology companies in the PRISM slides were keen to stress they do not go beyond what they are forced to do under law in handing over user data, but other documents suggest some internet and telecoms companies on occasion go beyond what is mandatory.
   2. Such relationships create issues of customer trust for US and UK technology giants, as Facebook founder Mark Zuckerberg publicly acknowledged, as well as raising questions as to whether what the law allows represents the limits of surveillance, or merely a starting point.
   3. Oversight for the NSA comes from the Foreign Intelligence Surveillance Court, which operates in secret. In the wake of the Snowden revelations, there has been widespread public and congressional pushback against the court’s efficacy, leading Obama to consider reforms to its operations and to declassify hundreds of pages of rulings from the court.
5. Recommended changes
   1. Henningsen, 2014
      1. Despite the size and scope of Edward Snowden's NSA whistleblowing, there's little sign of Washington DC changing its practices, and even less of an indication that any of its European allies will actually hold it to account.
      2. Herein resides the key aspect in all of this - that in order for agencies like the NSA and GCHQ to get easy access to all of our digital communications and data, they still need the cooperation of corporations to do it. In the US, it’s now known what role major ISPs and mobile carriers like Verizon and AT&T play in this equation within US borders, including the existence of NSA-controlled SG3 collection rooms embedded within the companies facilities. Shocking enough, but not nearly as shocking if you consider the role of transnational corporations in enabling the NSA access to your digital threads.
      3. Internationally, citizens have already signed over most of their privacy simply by using the digital services of US multinationals like Google, Facebook, Apple, Microsoft, Skype, Yahoo and others. All of these corporation operate within a ‘profit-first’ ethical vacuum where, in many cases, they are actually charging the NSA for the privilege of consuming their customers’ communications and data. According to the recent Snowden leaks, the level of collusion between Microsoft Corp and the NSA is astonishing, where Microsoft allows the NSA to skirt encryption protocols on Outlook, Skype video and cloud services, and where data captured by the NSA is routinely passed on to both the FBI and the CIA (Guardian July 12, 2013).
      4. The horrible irony here is too obvious to ignore: the US government, through its NSA, is giving away taxpayer dollars so these corporations can profit from handing over all of your personal communications and data. Such an unholy alliance between partnering governments and transnational corporations could be defined as fascism, but the global nature of this operation might require a new term to define what means as a global phenomenon.
      5. Amidst the international Snowden media circus, it’s important not to forget that what has enabled agencies like the NSA and GCHQ to act with impunity, is the fact that both these governments have excelled in capitalising on a post-September 11th paranoia that has hijacked the national consciousness in both the US and the UK. The entire basis upon which their relentless war-time remit has been erected can be described in three words: “War on Terror”.
      6. It’s already clear to the global citizenry that the US federal government and its NSA are out of control, and should be reined in as soon as possible in order to preserve any remaining moral standing for a country which has exhausted nearly all of its goodwill internationally – as well as domestically.
      7. Judging by Washington’s stoic and unapologetic stance thus far, goodwill doesn’t seem to be a high priority yet. Until the problem is properly addressed, there will remain a gaping hole of moral leadership in the international community.
      8. What political leaders are slow the realize is that when the goodwill has been exhausted, so has the trust, and that’s a very slippery slope indeed.
   2. My opinion.
      1. Once a government program has been started, it never stops. I’ve never known of any government program that ended. As Ronald Reagan stated in his speech “A Time for Choosing”, “No government ever voluntarily reduces itself in size. So governments' programs, once launched, never disappear.”
      2. More oversight and transparency.
6. Conclusion
   1. Thomas Jefferson, who authored the United States Declaration of Independence and was our country’s third president, famously stated, “the price of liberty is eternal vigilance”. This still holds true to this day.

References:

Bailey, R. (2013) ‘Open Letter to Obama and Congress From Internet Giants Calls For Reining In Government Surveillance’, *Reason.com* [Online]. Available from: <http://reason.com/blog/2013/12/09/open-letter-to-obama-and-congress-from-i> (Accessed: 24 May 2014)

The Guardian (2014) ‘The NSA Files’, *The Guardian* [Online]. Available from: <http://www.theguardian.com/world/the-nsa-files> (Accessed: 24 May 2014)

Henningsen, P. (2013) ‘NSA is more than just a spy network, it’s global fascism’, *Russia Today* [Online]. Available from: <http://rt.com/op-edge/nsa-network-global-fascism-167/> (Accessed: 24 May 2014)

Kelly et al. (2013) *Freedom on the Internet 2013: A Global Assessment of Internet and Digital Media* [Online]. Available from: <http://www.freedomhouse.org/article/new-report-internet-freedom-deteriorates-worldwide-activists-push-back#.U4EIIRaI3Ro> (Accessed: 24 May 2014)

Kloc, J. (2013) ‘The Definitive Guide To NSA Spy Programs’, *The Daily Dot* [Online]. Available from: <http://www.dailydot.com/politics/nsa-spy-prgrams-prism-fairview-blarney/> (Accessed: 24 May 2014)

Ronald Reagan Presidential Foundation & Library (2009) *A Time for Choosing*, [Youtube Video, Online]. Available from: <https://www.youtube.com/watch?v=qXBswFfh6AY> (Accessed: 24 May 2014)