Comparison of roles and responsibilities of the australian government

ASSIGN BUSTER

Compare and contrast the respective roles and responsibilities of the Australian government, businesses and individuals in maintaining data privacy.

Our society is becoming increasingly dependent on our access to our online data. Almost all aspects of our lives have some sort of record kept online. From our financial information to our health records, everyone has important data that needs to be secure online. With this increased dependence on our online presence, data security is of the utmost importance. The responsibility for data security largely remains on the businesses and governments of our society to ensure individuals data is secure. This essay will argue that, while the government, businesses and individuals all play a role in data security, it is a major responsibility of large companies and the government to ensure data security is a priority. While individuals can only do so much to ensure their data is secure. Establishing secure passwords, regularly changing passwords and using words that cannot be found in the dictionary are measures that individuals can take to secure their data. Beyond these methods, it is largely out of their hands. Businesses are responsible for maintaining individual’s data security. Large companies such as social media, health services and banks all hold massive amounts of sensitive information and have added responsibility to retain data security. The government of Australia is responsible for ensuring that data leaks are prevented at all costs for to protect citizens and for national security purposes. The individuals that make up the government all play a role in maintaining data security.

Individuals have a lot to lose when it comes to data security. Throughout the internet there is stored records of everyone’s health history, bank details and even employment history. The standard for security of online systems being a simple password that grants access to a user’s information. In order to maintain data security for individuals, there must be a secure password put in place to prevent any unauthorised users from guessing the password. But many fail to do so. Users often duplicate the same password to use for multiple accounts across the internet. “ While research supports the frequent changing of passwords to reduce predictability, this study found that 79. 6 percent of the surveyed users said they never changed their password.” (Zviran and Haga, 1999, p. 12) On top of users reusing the same password in multiple places, many fail to realise that using a normal word that can be found in the dictionary as a password puts your data security at risk. ‘ The problem with using passwords that are derived directly from obvious words is that when a user thinks ‘‘ Hah, no one will guess this permutation,’ they are almost invariably wrong.” (Klein, n. d., p. 6) This is because accounts can be cracked by using a program that attempts to log into an account by trialling every word in the dictionary. A password that ensures data security must be a combination of letters, numbers and special characters. Data security is the responsibility of the individual to ensure passwords are secure, changed regularly and are not reused in multiple locations, however, other than this there is not much more a user can do to guarantee data security. Data can still be leaked despite individuals’ best efforts. Despite these differences, the responsibility to maintain data security is similar between individuals and businesses/governments. The individuals that make up these larger organisations that hold much more sensitive data relies on

the data security practices of individuals. The very first measure that governments and businesses must take to ensure data security is to educate all individuals within these organisations on basic data security.

Businesses have the most responsibility when it comes to ensuring their data is secure. Banks and medical services all hold extremely sensitive data from a massive amount of people. Data such as financial details and health records are all confidential and failure to secure the data could lead to thousands of people being at risk. Data collected from these businesses is also a very valuable resource, as it can be sold to other businesses for marketing purposes. “ Soon after you tell your doctor about an intimate medical problem, data about your condition are sold commercially to companies that have nothing to do with your treatment or billing” (Tanner, 2017, p. 1). It is the responsibility to ensure that the selling of this data is ethical and protects the privacy of the individuals. De-individualisation and encryption are two ways businesses can ensure that they protect the privacy of the individuals and ensure data is secure. De-individualisation is the removal of any information that can link data to a person, such as names and addresses which protects the identity of the business’ clients. Data encryption is a way of securing data “ Data encryption translates data into another form, or code, so that only people with access to a secret key (formally called a decryption key) or password can read it.” (Lord, 2015). The ways businesses can ensure their data is similar to how individuals can secure their passwords, however, they differ in how both individuals and businesses use this data. Individuals use their data as a way to manage their lives with bank data and health records, but many large companies collect

this data in order to store it for their own use. “ Online dating services, like Match. com, constantly sift through their Web listings of personal characteristics, reactions and communications to improve the algorithms for matching men and women on dates” (Lohr, 2012). Social medias are the companies that hoard the most data “ Social media companies collect so much data even they can’t remember all the ways the surveil us”(Leetaru, 2018). The responsibility for data security on businesses is not very similar to how individuals need to secure their data, but the government and the large businesses share many similarities in how they are responsible for securing data for thousands of citizens.

Much like businesses, the government stores sensitive data for thousands of citizens from things such as legal records to tax information. It is the responsibility of the government to ensure this data is secured to protect the citizens that this data refers to. With the government now using cloud solutions as a way of data storage (Paquette et al., 2010), it is the responsibility of the government to ensure measures are put in place to ensure data is secure. In a similar to how businesses should secure data through de-individualisation and encryption of data. But on top of this responsibility to ensure individuals data is secure, governments have the added responsibility of preventing leakage of data for national security purposes, which is not a responsibility of businesses. “ The work details of 30, 000 Victorian public servants have been stolen in a data breach, after part of the Victorian Government directory was downloaded by an unknown party” (ABC, 2019) The government has added responsibility of preventing leaks like this, because having sensitive data such as “ work emails, job titles

and work phone numbers.” (ABC, 2019) leaked puts national security at risk. “ The dataset as a whole could be useful for a more targeted attack.” (ABC, 2019) This separates the responsibilities of governments from businesses as a severe data leak from the government puts the entire country at risk, whereas a data leak from a business will only effect those associated with the business. The consequences of a data leak are much more damaging for governments than it is for businesses and individuals.

Despite the higher consequences for government data leaks, it is the individuals that make up the government have a responsibility to maintain data security for the government. Government officials must take precautions for data security that also apply to regular individuals such as updating passwords and not re-using them in multiple places. Failure to meet these basic methods of maintaining data security could put sensitive government data at risk.

While individuals, businesses, and governments share some similarities in data security, businesses and governments have a much larger responsibility to maintain data security as the consequences of a data breach are far more severe for businesses and governments compared to an individual. Individuals can maintain their data security by establishing secure passwords and regularly changing them whereas businesses and governments have a responsibility to encrypt and de-individualise data in order to protect individuals and prevent data leaks from occurring. Businesses and governments differ in that a leak from the government can place an entire country’s security at risk whereas a business leak only effects those affiliated with the business. Individuals, businesses and governments all require a

level of data security, however, governments and businesses have more of a responsibility than individuals to ensure that data leaks are prevented. In this society of growing dependence on technology, maintaining data security and privacy is a genuine concern as the internet becomes a progressively more cluttered system with incomprehensible amounts of information stored on it.

- ABC, 2019. Victorian Government employees' details stolen in data breach [WWW Document]. ABC News. URL https://www. abc. net. au/news/2019-01-01/victorian-government-employee-directory-data-breach/10676932 (accessed 5. 27. 19).
- Klein, D. V., n. d. '" Foiling the Cracker"': A Survey of, and Improvements to, Password Security 11.
- Leetaru, K., 2018. Social Media Companies Collect So Much Data Even They Can't Remember All The Ways They Surveil Us [WWW Document]. Forbes. URL https://www. forbes. com/sites/kalevleetaru/2018/10/25/social-media-companies-collect-so-much-data-even-they-cant-remember-all-the-ways-they-surveil-us/ (accessed 5. 28. 19).
- Lohr, S., 2012. Big Data's Impact in the World – The New York Times [WWW Document]. URL https://www. nytimes. com/2012/02/12/sunday-review/big-datas-impact-in-the-world. html (accessed 6. 4. 19).
- Lord, N., 2015. What Is Data Encryption? Definition, Best Practices & More [WWW Document]. Digit. Guard. URL https://digitalguardian. com/blog/what-data-encryption (accessed 5. 28. 19).

- Paquette, S., Jaeger, P. T., Wilson, S. C., 2010. Identifying the security risks associated with governmental use of cloud computing | Elsevier Enhanced Reader [WWW Document]. https://doi. org/10. 1016/j. giq. 2010. 01. 002
- Tanner, A., 2017. Our Bodies, Our Data: How Companies Make Billions Selling Our Medical Records. Beacon Press.
- Zviran, M., Haga, W. J., 1999. Password Security: An Empirical Study. J. Manag. Inf. Syst. 15, 161–185. https://doi. org/10. 1080/07421222. 1999. 11518226