"Privacy is over. Get used to it" is often attributed to Scott McNealy, former CEO of Sun. Is he right?

Karthikeya Udupa K M (1393456)

October 31, 2013

Privacy is defined as "A state in which one is not observed or disturbed by other people" by the Oxford dictionary and in a general scenario it usually relates to the autonomy and secrecy of the user. In reference to the web, privacy usually refers to personal information and the invasion of privacy is usually interpreted as the unauthorised collection, disclosure, or other use of personal information as a direct result of electronic commerce transactions (Wang, Lee, and Wang 1998). Since the last two decades we have seamlessly connected the world through the world throughout world wide web but in the process have opened up multiple ways of privacy evasion. We have made efforts to building secure and robust systems, but massive security and privacy failures that occur time and again (Armerding 2012), have proved that privacy might just be a paradox.

The privacy paradoxical state can partially be attributed to the fact that the web has become so immense, that the user tends to use products and services that accumulate his personal information, the company providing these services might have a relaxed approach towards the information's security, giving an opportunity for privacy failures waiting happen (Markowitz 1999). This also provides the authorities a medium monitor the user's actions and communications which (Clarke 1988) defines as "dataveillance". The rise in the usage of social networks, especially among teenagers, wherein they disclose accurate personal information online (Acquisti and Gross 2006) has been a primary privacy concern (Barnes 2006; Young and Quan-Haase 2009). Emergence of ubiquitous, physiological and location aware systems have taken privacy concern to a different dimension, not only does the user have to be concerned with data security but now information such as his location (Wang and Liu 2009), medical conditions, which in some cases he might not be aware of (Fairclough 2009), etc may be compromised. The problem, it turns out might not just be developing a secure system and user keeping a vigil on his information, there are various other factors such as market dynamics

and political influences that govern the privacy standards (Anderson 2001). Also, not everyone shares the same views on privacy, certain authorities have been making even further attempts to curb the user's privacy (113th Congress 2013; 112th Congress 2011).

Security techniques are being constantly upgraded to handle the information more securely. Law's have been passed by government authorities in many parts of the world (OECD 1988; Govt. 1998) to manage and regulate how the information being collected from the user and has been applied to public and in some cases private sectors although on the other hand privacy of the user is being compromised for security reasons. Although, amends have constantly been made to ensure upmost standards, privacy at present is a paradox, it is the price you pay if you are to consume services and use products today and at the end it falls on the user to take weighted decisions when dealing with critical personal information.

References

112th Congress (2011). Preventing real online threats to economic creativity and theft of intellectual property act of 2011. *https://www.govtrack.us/congress/bills/112/s968/text (Accessed 30th October 2013.)*.

113th Congress (2013). H.r. 624: Cyber intelligence sharing and protection act. *https://www.govtrack.us/congress/bills/113/hr624/text (Accessed 30th October 2013.)*.

Acquisti, A. and R. Gross (2006). Imagined communities: Awareness, information sharing and privacy protection on the facebook. In *6th Workshop on Privacy Enhancing Technologies*. Cambridge, UK.

Anderson, R. (2001). Why information security is hard-an economic perspective. In *Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual*, pp. 358–365. IEEE.

Armerding, T. (2012). The 15 worst data security breaches of the 21st century. Technical report.

Barnes, S. B. (2006). A privacy paradox: Social networking in the united states. *First Monday 11*(9).

Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM 31*(5), 498–512.

Fairclough, S. H. (2009). Fundamentals of physiological computing. *Interacting with computers 21*(1), 133–145.

Govt., U. (1998). Uk data protection act 1998. *http://www.legislation.gov.uk/ukpga/1998/29/contents (Accessed 30th October 2013.)*.

Markowitz, M. (1999). You have no privacy. *ProQuest 44*(7), 20.

OECD (1988). Oecd guidelines on the protection of privacy and transborder flows of personal data. *http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborde (Accessed 30th October 2013.)*.

Wang, H., M. K. Lee, and C. Wang (1998). Consumer privacy concerns about internet marketing. *Communications of the ACM 41*(3), 63–70.

Wang, T. and L. Liu (2009). From data privacy to location privacy. In *Machine Learning in Cyber Trust*, pp. 217–246. Springer.

Young, A. L. and A. Quan-Haase (2009). Information revelation and internet privacy concerns on social network sites: a case study of facebook. In *Proceedings of the fourth international conference on Communities and technologies*, pp. 265–274. ACM.