Ian Coffey, Brendan Lewis

Computer Networks & Security

Capt. Rashly, USMC

25 January, 2025

Five Eyes

Ever since the NSA Snowden leaks in 2013, the world has been under no illusion as to the capabilities of western intelligence agencies. From hacking foreign heads of states to wiretapping millions of mobile phones all around the world, the capabilities of the NSA have skyrocketed into a league of its own, for better or for worse. Not all NSA targets are foreign adversaries either. Alongside other revelations, the Snowden leaks unveiled how the NSA tapped into Googles GFE’s, or Google Frontend Servers (Anderson 38). When internet traffic is routed towards Google servers, it is encrypted all the way until it reached a GFE. Once the traffic is within Googles own network, it is transmitted as plaintext. Since the NSA tapped into GFE’s, they didn’t even have to perform any decryption, all the data that Google received and handled was plain to see for anyone who was watching, even those who Google didn’t think was watching. This immense amount of data that was tapped into fed into an even larger project, XKeyscore. In short, using the data that the NSA collected, XKeyscore was a database constructed to return the relevant and personal information regarding anyone and everyone that the NSA had spied on (Anderson 41). In short, if you typed in someone’s name into XKeyscore, a screen showing their phone number, email, residency, job, contacts, what phone they have, their internet service provider, and much more would appear. XKeyscore and its vast amount of data and insight was used in the capture of three hundred al-Qaida terrorists (Anderson 41). However, the toolbox of the NSA does not stop there. Tools like Long Haul can defeat VPN obfuscation of internet traffic, Quantum can brute force 1024-bit Diffie Helmen encryption, and malware like Stuxnet has proved how powerful and destructive state sponsored cyber warfare can be. In an ever-growing world, technology will only become more seeded into our everyday lives. With this in mind, the expansion of the cyber domain will lead in the expansion of cyber warfare, and western intelligence agencies have proved ready and capable of leverage cyber to achieve national security interests. Now the only question that remains is the same question that Edward Snowden had in the early twenty tens; Are we okay with all of this?